CYLAN VPN 用户手册

目录

一、 Cylan产品介绍……2
二、 Cylan配置向导……4
三、 Cylan首次安装配置……5
四、 Cylan Internet上网配置……7
连接Modem设备……
选择上网方式……
设置PC上网参数……
五、 Cylan远程拨号配置……13
拨入设置……
拨入账号设置……
远程用户设置……
六、 Cylan网络配置……16
IP地址配置……
DHCP配置……
高级网络配置……
七、 Cylan防火墙配置……19
外来访问……
包过滤……
防火墙规则……
入侵检测……
接入控制……
八、 CylanVPN配置……27
PPTP VPN客户……
PPTP VPN服务器……
IPSEC……
L2tp VPN 客户……
L2tp VPN服务器……
GRE……
九、 Cylan系统……36
时间服务器……
口令……
诊断……
高级……
十、 系统日志……39
访问日志……
管理访问日志……
自定义日志……
十一、Dynamic dns(动态域名解析)申请和使用……41
附录：常见网络问题解决方法……43

一、Cylan 产品介绍

Cylan 产品防火墙功能可以让用户的网络安全地连到 Internet 上，Cylan 防火墙提供全状态检测功能，可保护用户网络内的电脑不受外网黑客的攻击，同时也可检测数据包，以阻止未授权的访问；

Cylan 防火墙的 NAT 功能可以隐藏用户内网的 IP 地址，使用户可以安全地访问 Internet 网，同时 Internet 网的用户无法访问到用户电脑的资源；

Cylan 产品也提供 IPSEC、PPTP 服务器/客户端、L2tp 服务器/客户端和 GRE 等多种 VPN 功能；

下面是 Cylan 产品的网络安装简图：

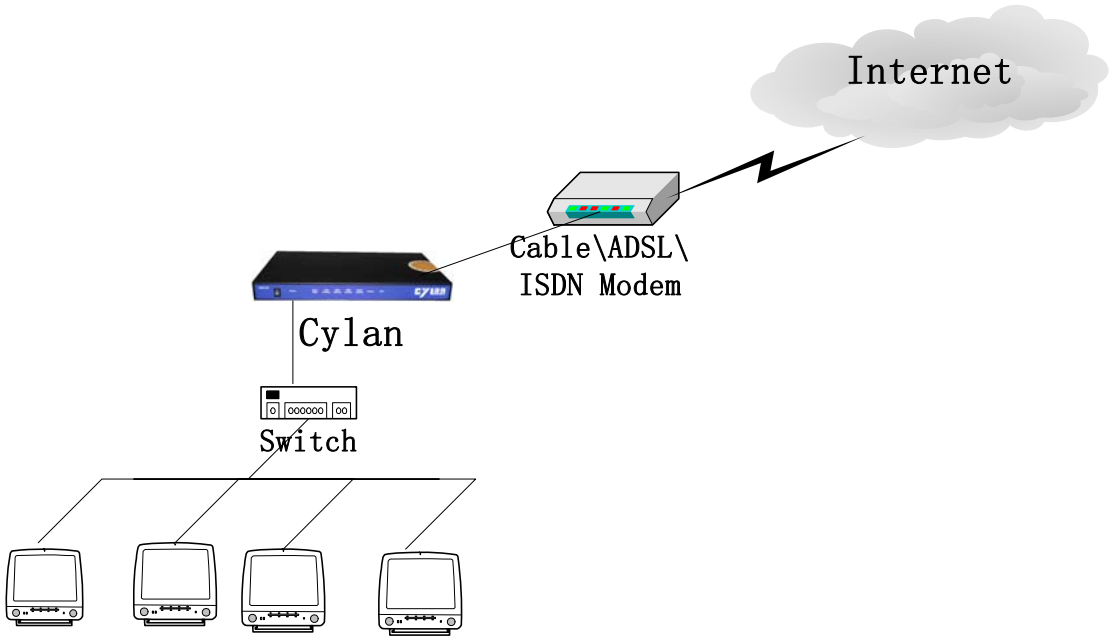


图 1-1

所有Cylan产品运行在一种安全的全状态检测防火墙下；在防火墙默认的工作方式下，只要用户的电脑连到局域网内，该电脑就可以访问到Internet,而电脑上的文件共享和Web应用服务等在没配置Cylan防火墙时，Internet用户是不能访问的；要开放这些服务请看后面的防火墙配置细节。

Cylan 设备的前面板指示灯如下图：

图 1-2

注意：

图 1-2 的指示灯在不同型号的产品的前面板，会有一些不同

指示灯的名称	指示灯的状态	指示灯状态的描述
Power	亮	设备已经供电
Heart Beat	闪烁	设备工作正常
	常亮或不亮	设备工作错误
LAN Activity	闪烁	在 LAN 接口有流量
WAN Activity	闪烁	在 WAN 接口有流量
DMZ Activity	闪烁	在 DMZ 接口有流量
Serial Activity	闪烁	在 Serial 接口有流量
Online	亮	Internet 已经连接成功
VPN	亮	VPN 已经被允许

设备的后面板包括一个 LAN 口、一个 Internet 口、一个 DMZ(高端产品如 SME500/500A 才有)、一个 COM1、一个电源口和一个 Reset 按钮;如下图：

图 1-3

后面板每个网口的状态指示灯有两个，下面的指示灯表示网线的连通状态（亮，表示连通），上面的指示灯表示网络流量，有流量，该指示灯会闪

环境参数

- **工作温度在0° C到40° C**
- **储藏温度在零下20° C 到 70° C**
- **湿度在0 到 95% (非浓缩)**

二、Cylan 配置向导

Cylan 的配置方法请看对应章节。

步骤	对应章节
Cylan 首次配置	第三章
Cylan 上网配置	第四章
Cylan 远程拨号配置	第五章
Cylan 网络配置	第六章
Cylan 防火墙配置	第七章
Cylan VPN 配置	第八章
Cylan 系统	第九章
Cylan 系统日志	第十章
Dynamic dns(动态域名解析)申请和使用	第十一章
常见网络问题解决方法	附录

三、Cylan 首次配置

1. **Cylan 设备通电，设备出厂时有一个默认 IP 地址：**
   IP 地址： 192.168.0.1
   子网掩码： 255.255.255.0

注意:
Cylan 设备在通电时，面板前面的灯会全闪（除了电源灯Power）;如果不全闪，在设备后面板上，可以3秒钟内连按2次reset按钮，把设备恢复到出厂配置

Internet 接口默认是没有激活的（如没有任何ip配置和dhcp服务配置）。

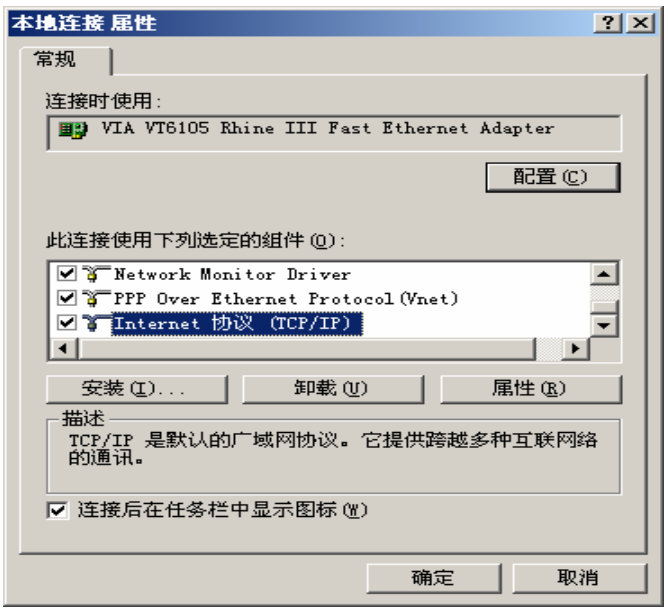
Cylan lan接口有一个默认ip 192.168.0.1

如果您把Cylan 设备连到带有DHCP Server的网络里，设备的lan接口将会自动获得一个ip地址

在配置Cylan设备之前，电脑需要一个和Cylan LAN接口在同一网段的IP地址；如果使用电脑直接连到Cylan LAN接口，用户可以使用包装中的交叉网线；如果把Cylan LAN直接连到HUB上，使用包装中的直通线

注意
建议用户使用电脑直接连到Cylan LAN接口；如果用户把Cylan 设备连到HUB上，用户网络中不能再有192.168.0.1这个地址

在电脑能和Cylan通信之前，用户必须修改电脑的网络配置
点 开始——〉设置——〉网络和拨号连接——〉本地连接——〉属性，如下图：



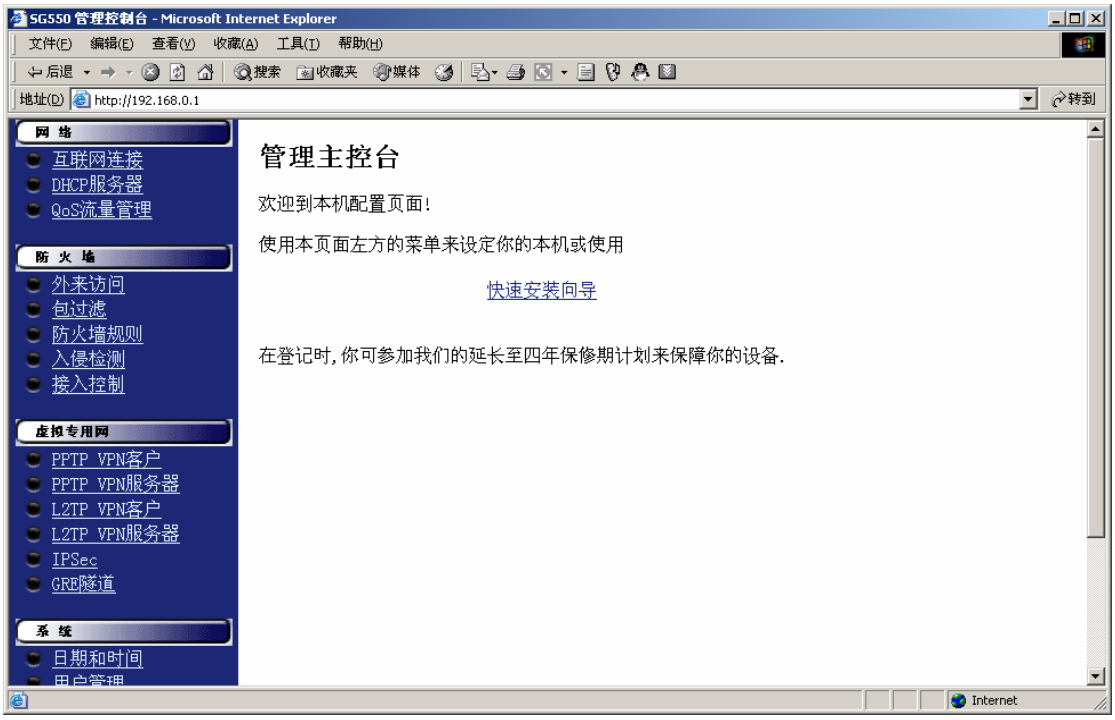
再选择**internet 协议(TCP/IP)**，点击 属性，如下图：

注意:

如果你需要保留你原来的IP地址，你可以在上图 高级 中再添加一个IP 192.168.0.2

2.设置 Cylan 的管理密码和 LAN IP

在 IE 地址中输入： 192.168.0.1 回车，您将看到下图：



在您点击上图任何文本链接时，Cylan 设备会提示您输入用户名和密码；你可以使用如下的默认的用户名和密码：
用户名：**root**
密码： **default**

注意：
如果不能打开上面的 Cylan 配置界面，或用户名和密码不接受,请在 3 秒内按 2 次后面板的 **Reset** *按钮(设备恢复到出厂设置)，再等 20-30 秒，再试着打开 192.168.0.1*

第一次配置 Cylan 设备必须修改密码才能进入其他参数的配置

四、Cylan 上网配置

1. 连接上网线路到 Cylan 设备
   56Kmodem、ISDN 和 CDMA 连到 Cylan 的 Serial 串口上;ADSL、Cable Modem 和 DDN、城域网连到 Cylan 的 Internet 口上。

2. 选择上网方式。
   点击 Cylan 配置界面的 互联网连接
   如下（以 ADSL 为例）：

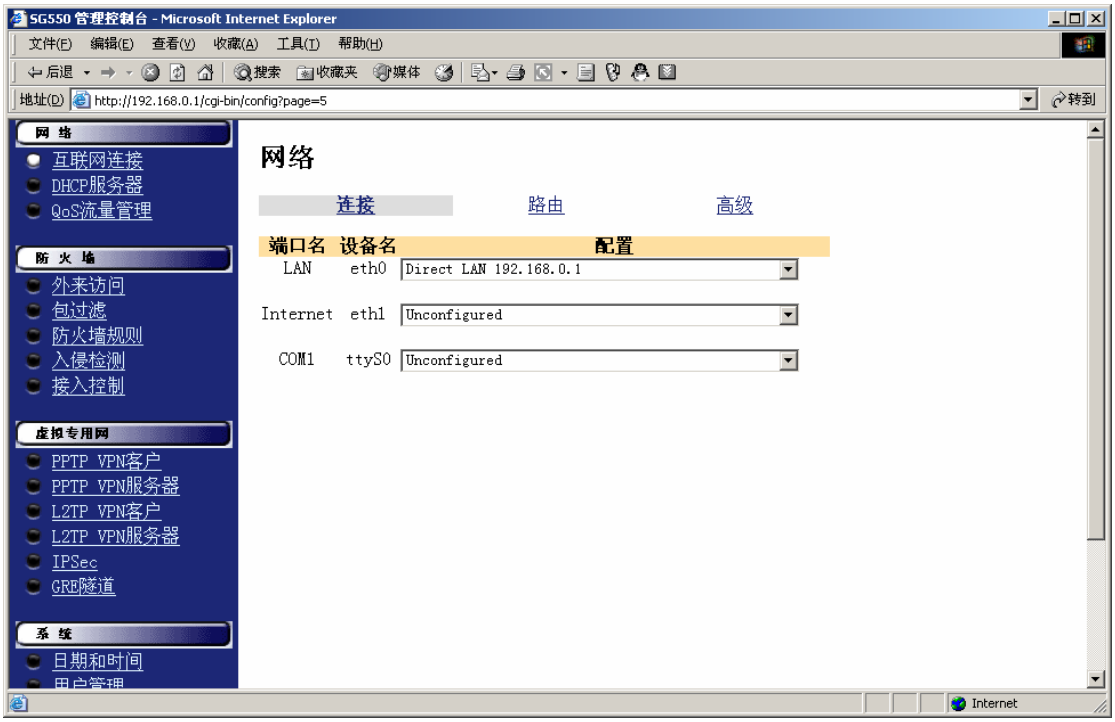


图 4-1

在图 4-1 中 **Internet eth1** 点击 **Unconfigured** 从下拉选项中 选择 改为 ADSL 上网，

如下图：

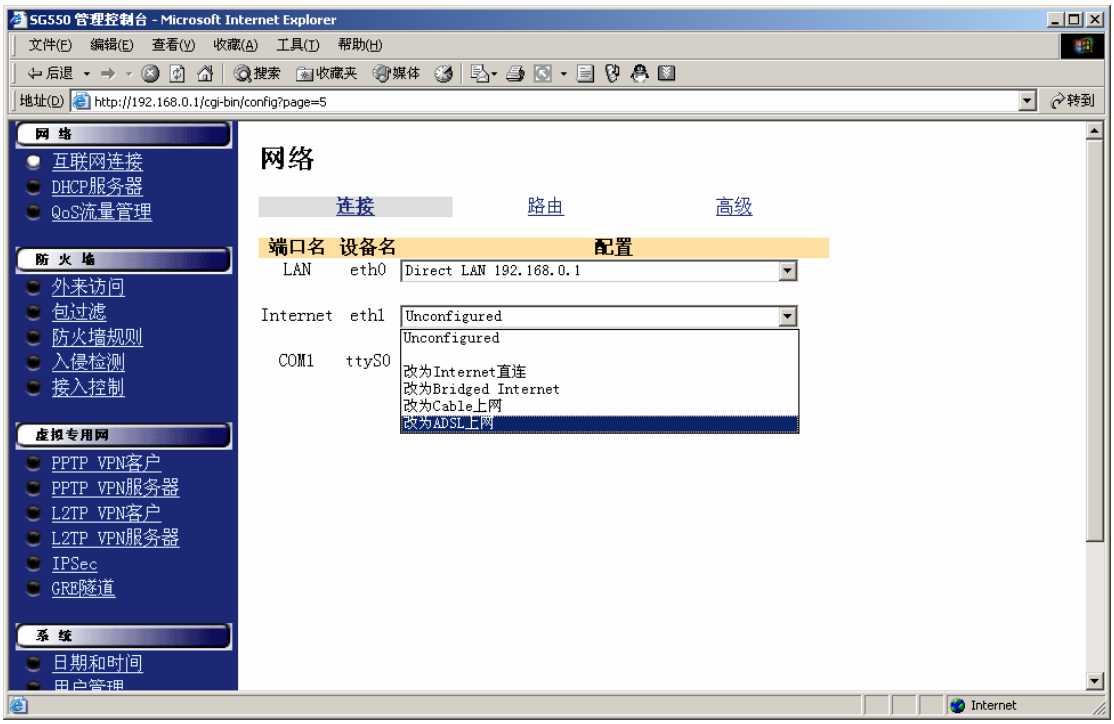


图 4-2

继续(下一步)：

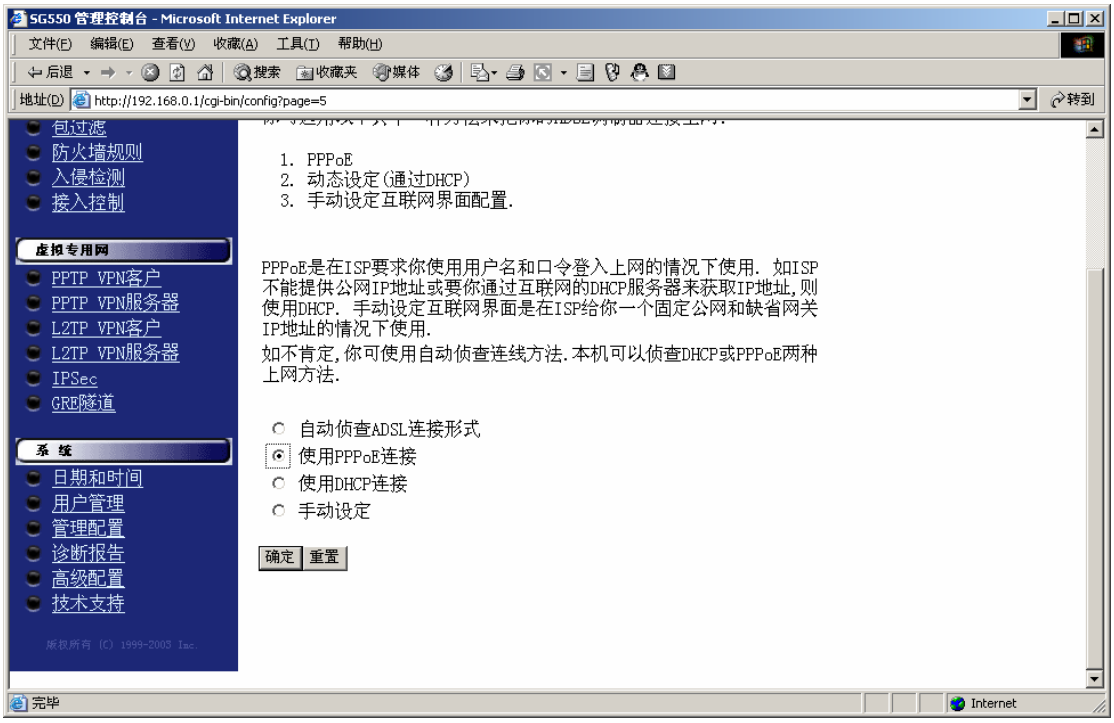


图 4-3

确定(下一步)：

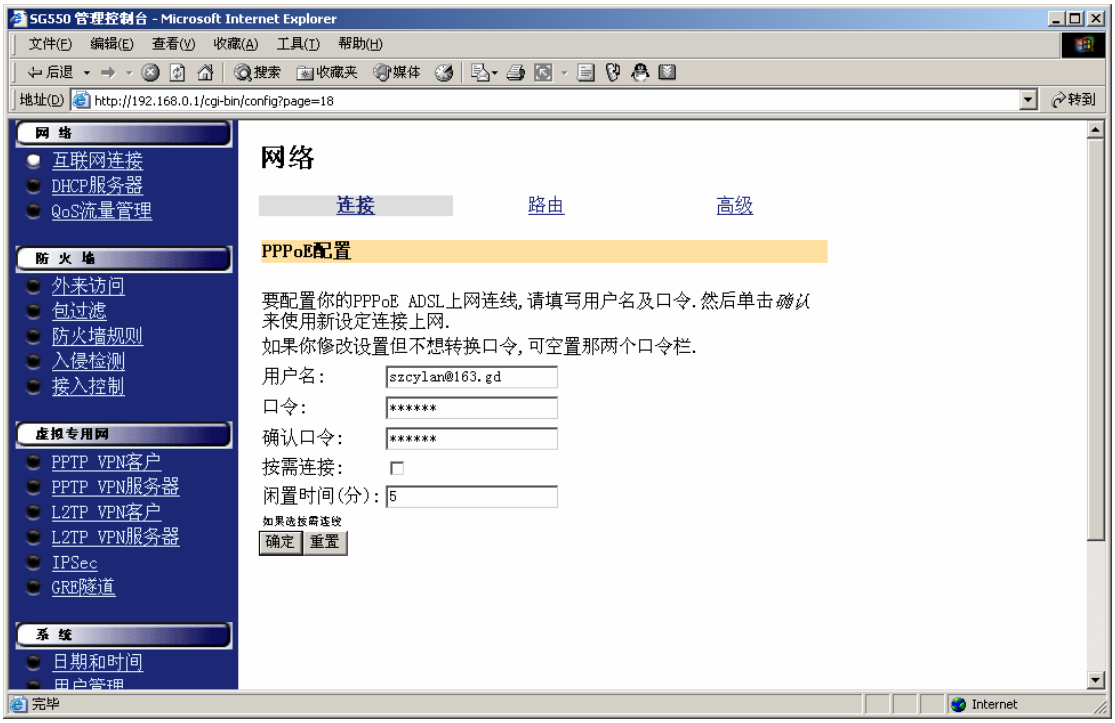


图 4-4

输入 ADSL 上网账号 参看图 4-4

确定(下一步):

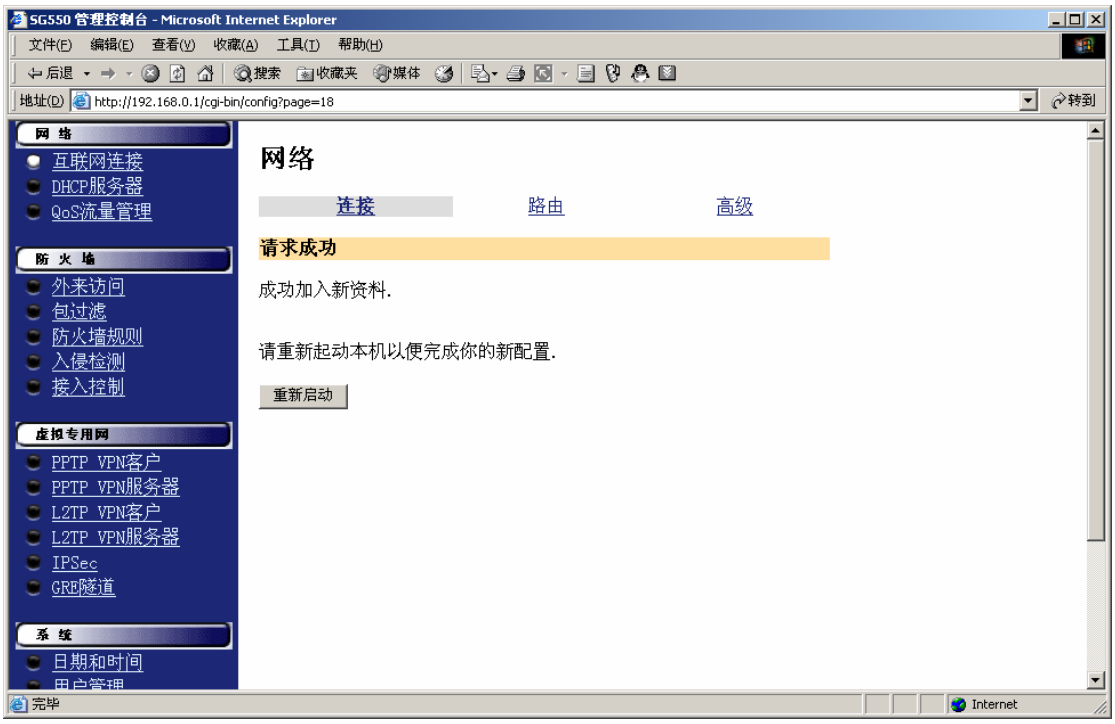


图 4-5

ADSL 账号添加成功，重新启动设备！参看图 4-5

2、Internet 直连上网配置

如果用户通过静态 IP 上网或 DHCP 方式上网，请参考下面的步骤：

点击　互联网连接——〉连接

选择　改为 internet 直连　　如下图：

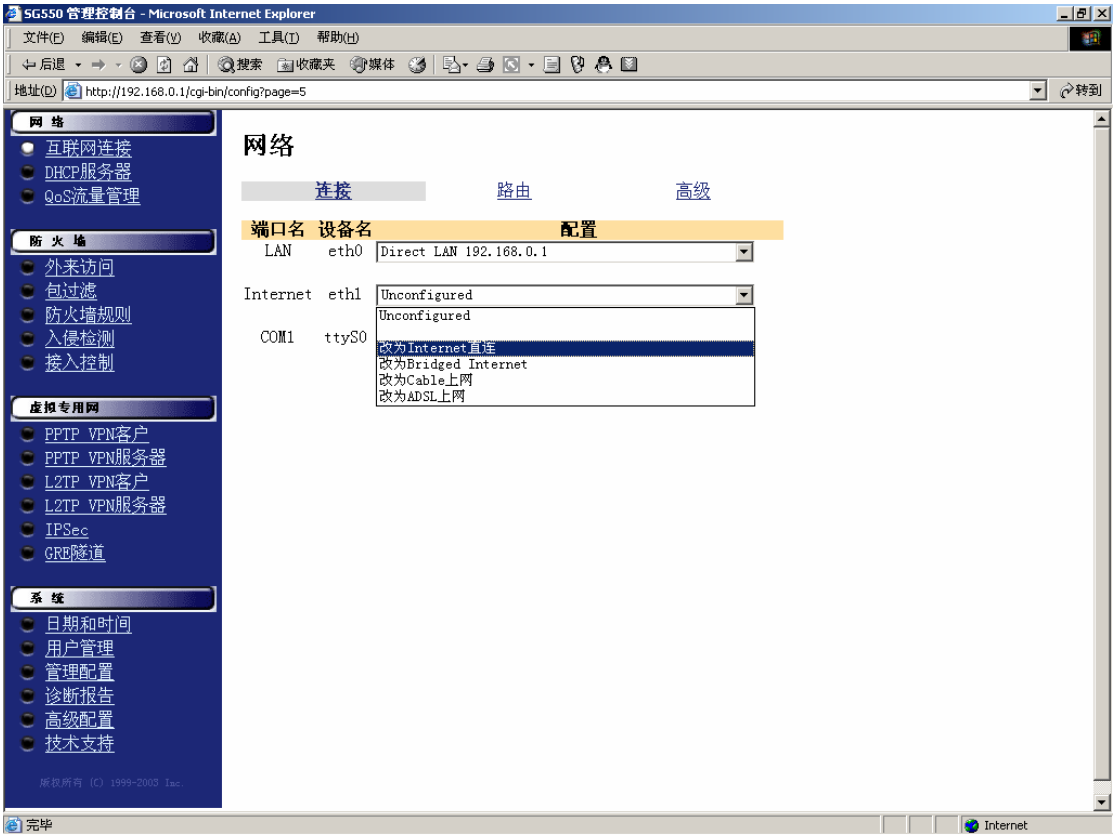


图 4-6

配置高级连线参数或自动备份切换连线.

选择. 改为 Dialout 上网备份　如　图 4-7

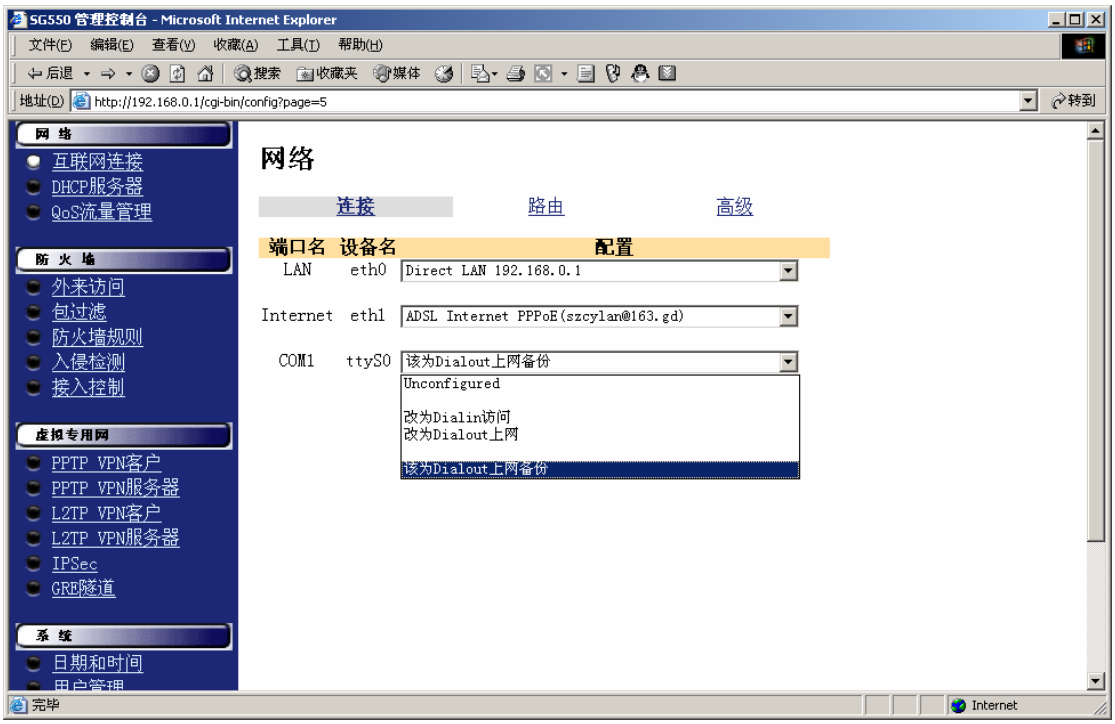


图 4-7

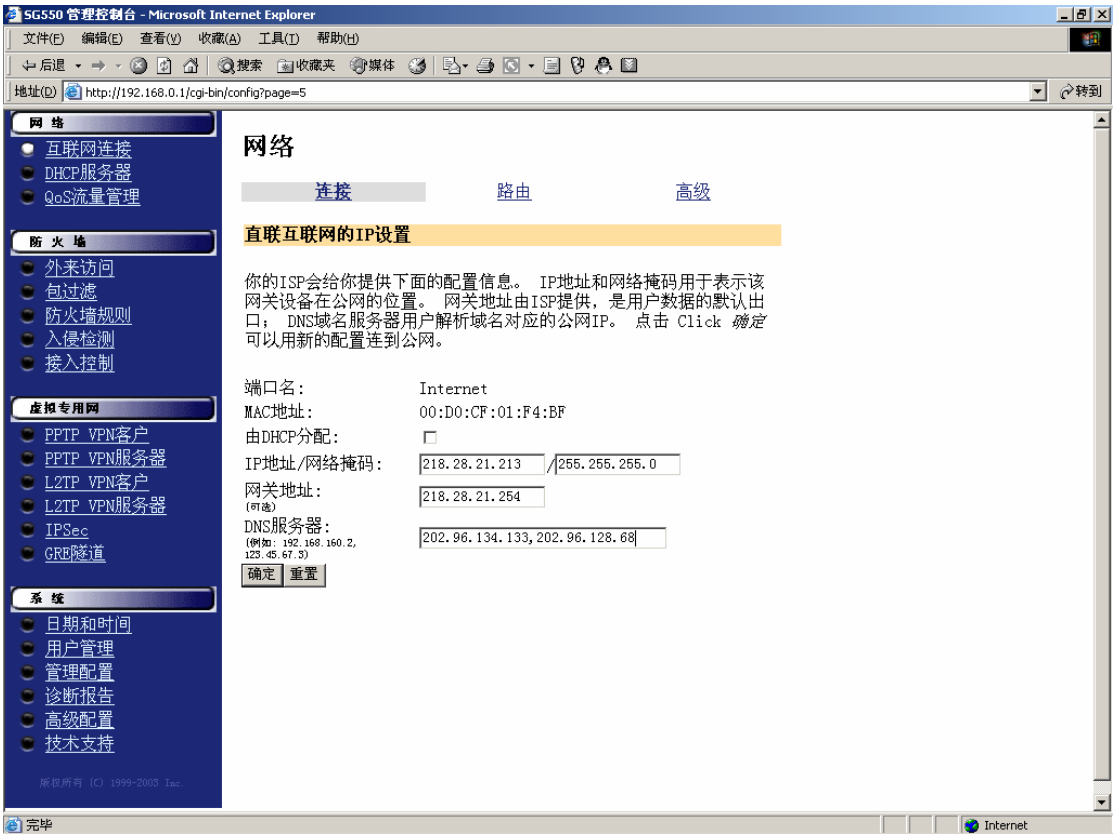


图 4-8

按图 4-8 中 确定 ，上网配置结束。

注意

图 4-7 是假设用户是静态 IP 上网；如果用户是 DHCP 上网，用户只要在图 4-7 中选中 由 DHCP 分配 *就可以了*

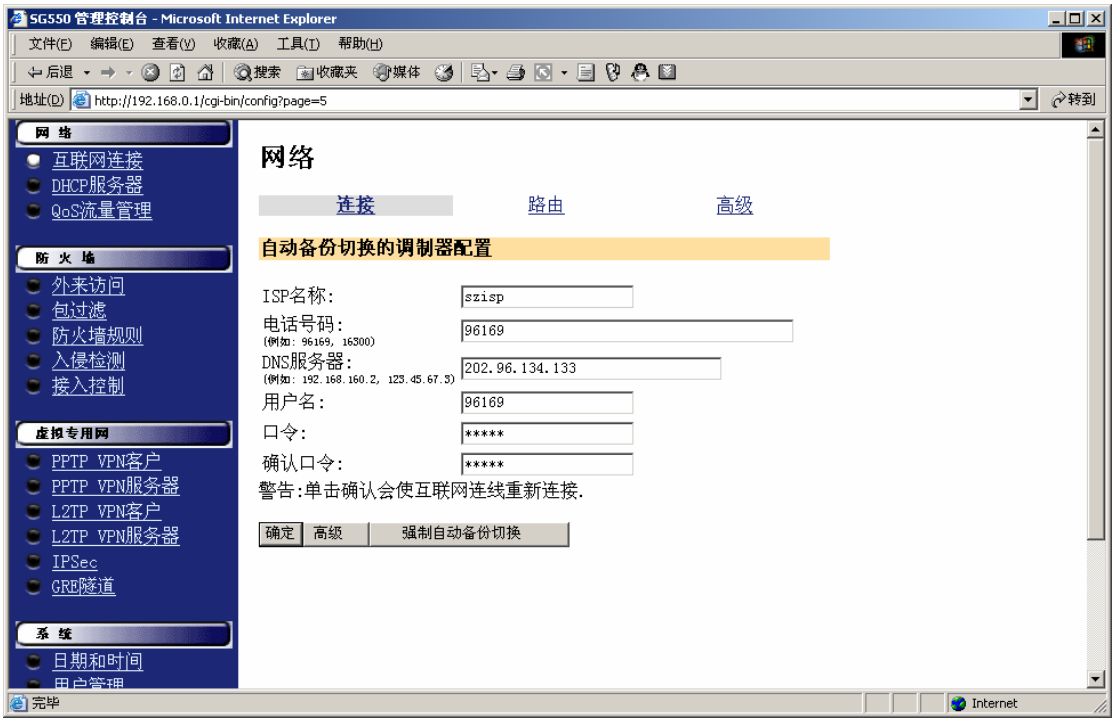


图 4-9

上面各栏不能为空；输入备份线路上网账号！

3. 设置 PC 上网方式。

在网上邻居属性的 TCP/IP 中设置。参看图 4-10

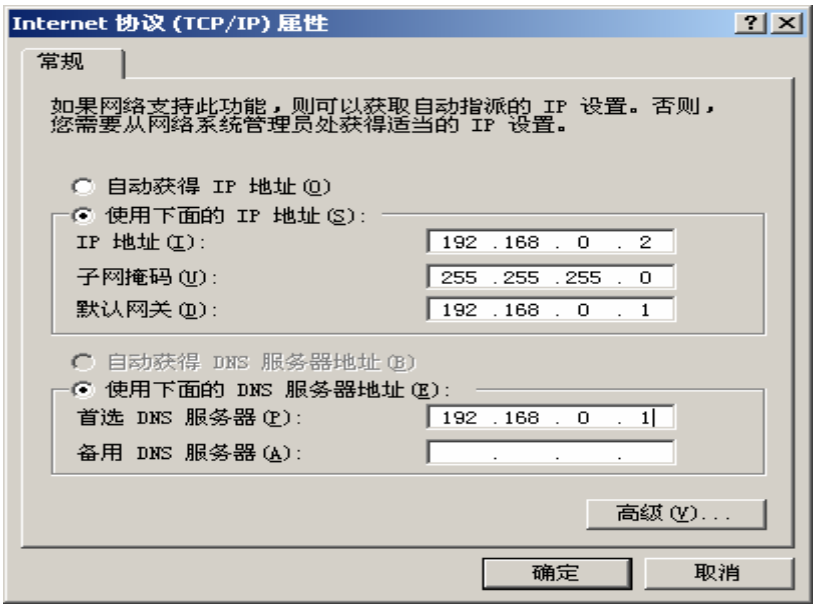

Internet 协议 (TCP/IP) 属性
常规
如果网络支持此功能，则可以获取自动指派的 IP 设置。否则，
您需要从网络系统管理员处获得适当的 IP 设置。
自动获得 IP 地址(O)
使用下面的 IP 地址(S):
IP 地址(I): 192 . 168 . 0 . 2
子网掩码(U): 255 . 255 . 255 . 0
默认网关(D): 192 . 168 . 0 . 1
自动获得 DNS 服务器地址(B)
使用下面的 DNS 服务器地址(E):
首选 DNS 服务器(P): 192 . 168 . 0 . 1
备用 DNS 服务器(A):
高级(V)...
确定
取消

图 4-10

五、Cylan 远程拨号配置

1. 点击 互联网连接——〉连接——〉COM1
   选择 COM1 口的 改为 Dialin 如图 5-1 所示连接 Modem,为远程用户分配 IP 地址和选择合适的验证方法；：

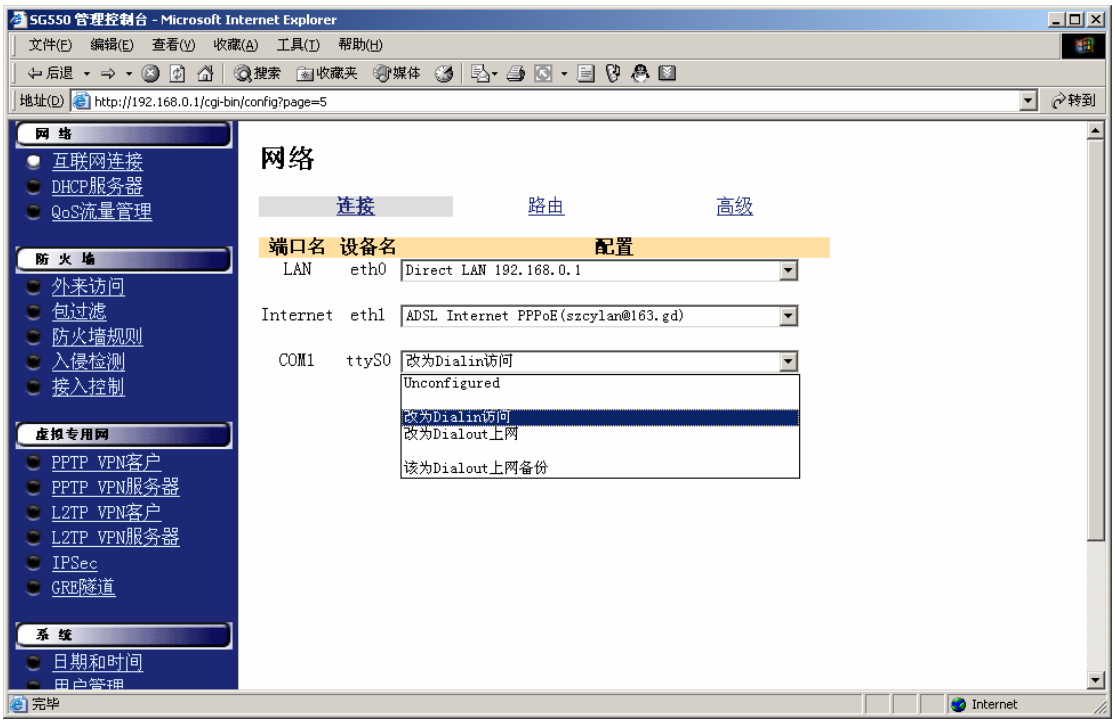


图 5-1

在图 5-1 中设置完后，继续(下一步)

2. 拨入账号配置

设置远程拨号账号 参看图 5-2

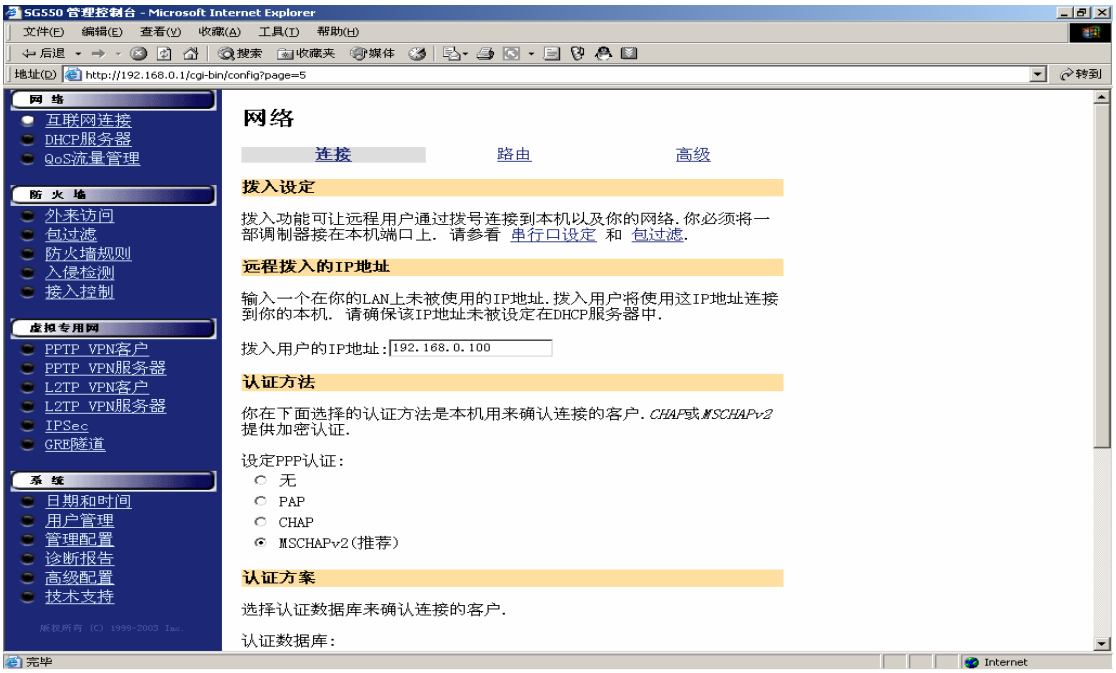
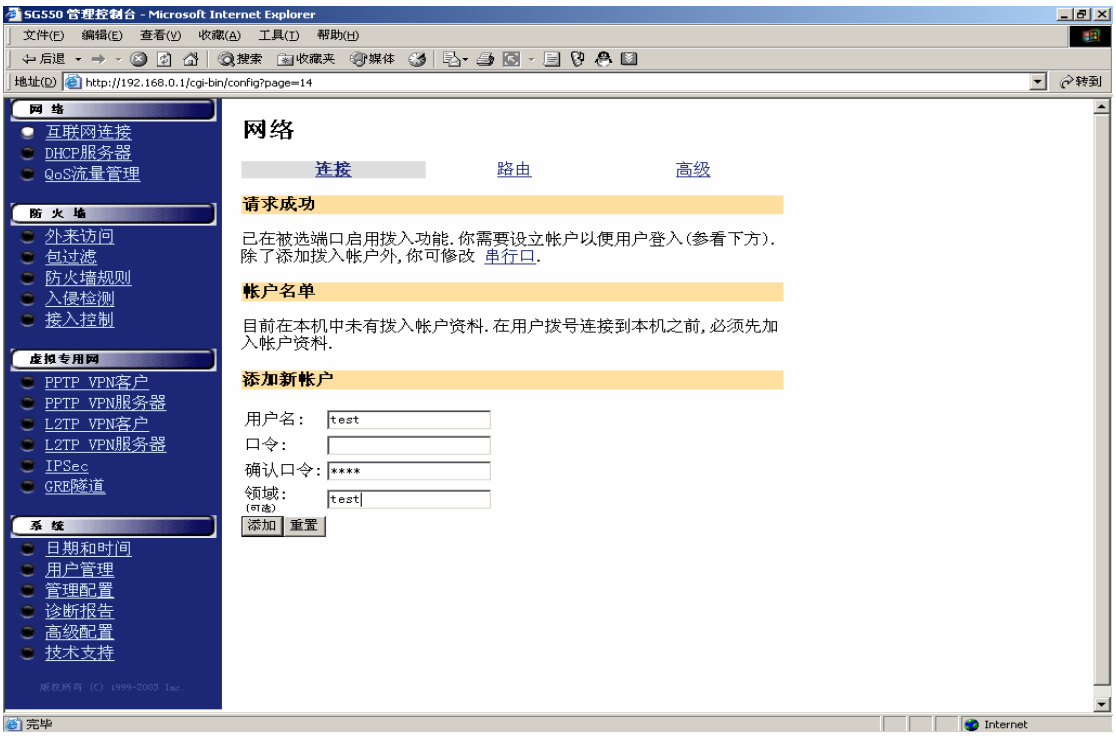


图 5-2

在图 5-2 中 按 继续 按钮



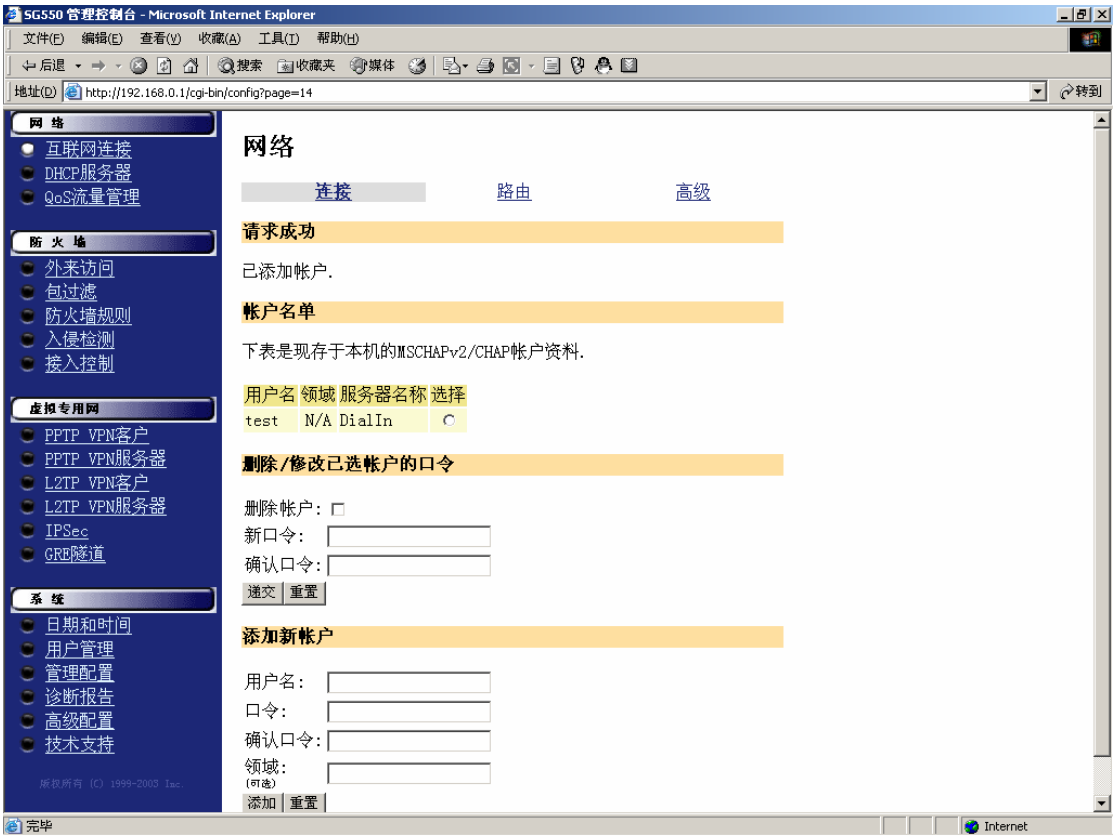


图 5-3

账号添加成功！参看图 5-3

3. 远程用户配置(略)

六、Cylan 网络配置

1、互联网连接 中的 IP 修改：参看图 6-1

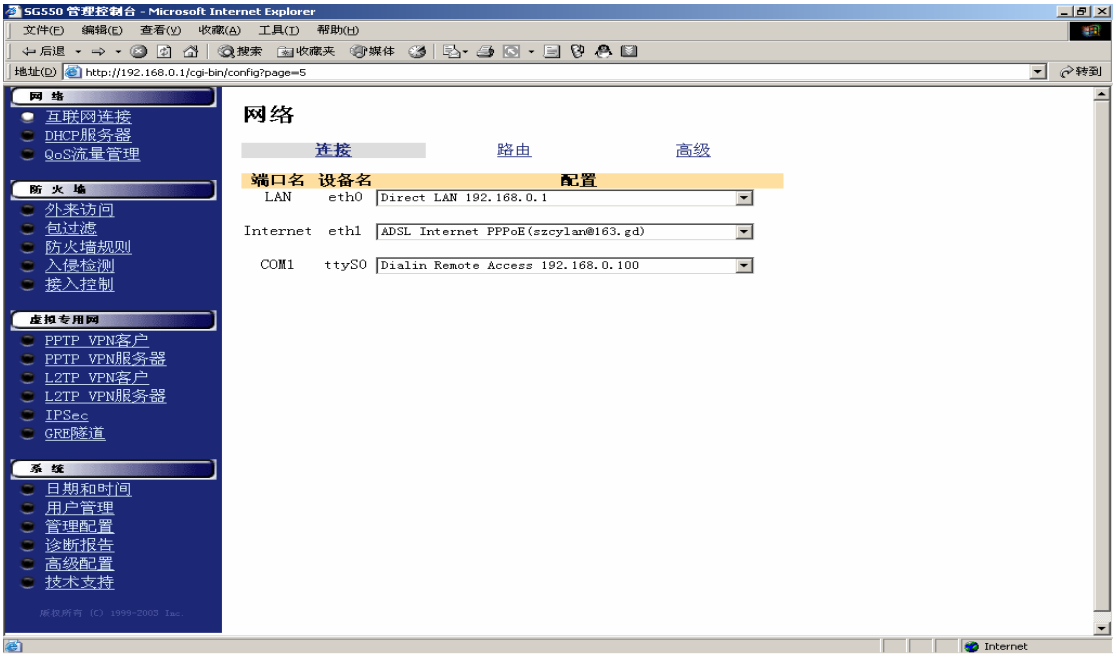


图 6-1

在 Lan eth0 界面处可以编辑局域网口地址，修改完 IP 后，这时系统会要求重新启动；
在 Internet eth1 界面中可以编辑上网方式

在图 6-1 高级 中，我们可以配置其他参数，如图 6-2：

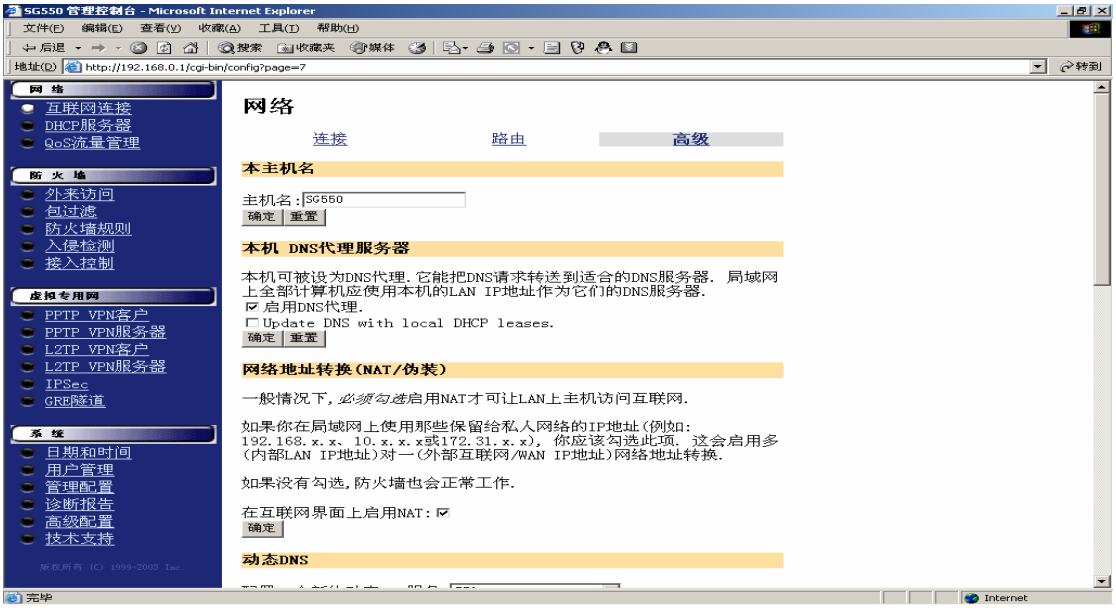


图 6-2

在图 6-2 中，Dynamic DNS 用于全动态 IP 建 VPN

2、DHCP 服务器：参看图 6-3

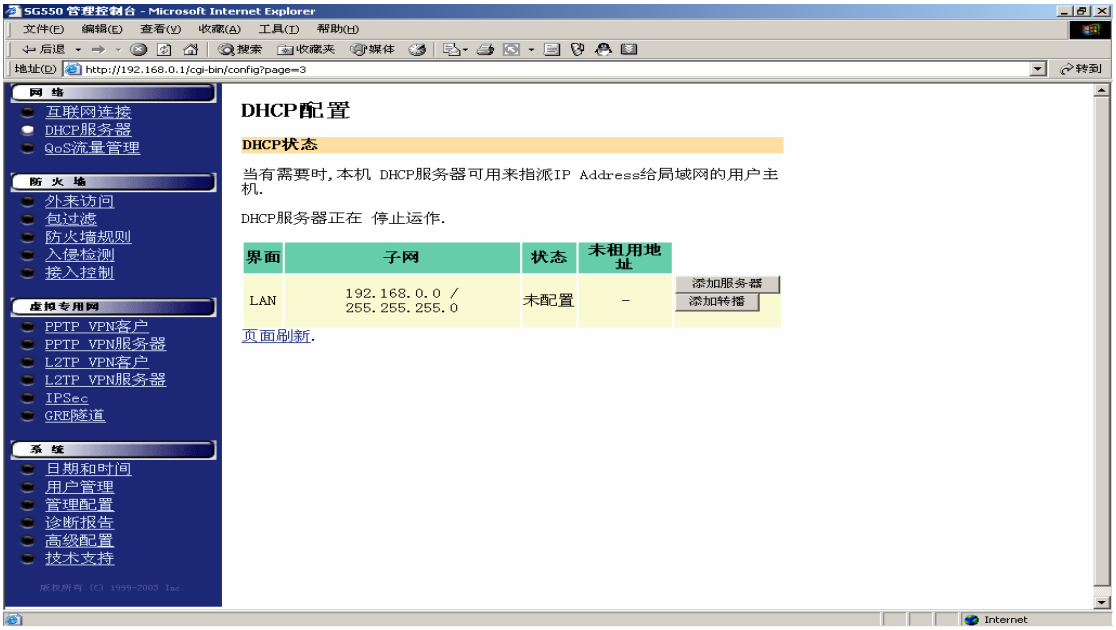


图 6-3

DHCP 参数设置，如图 6-4：

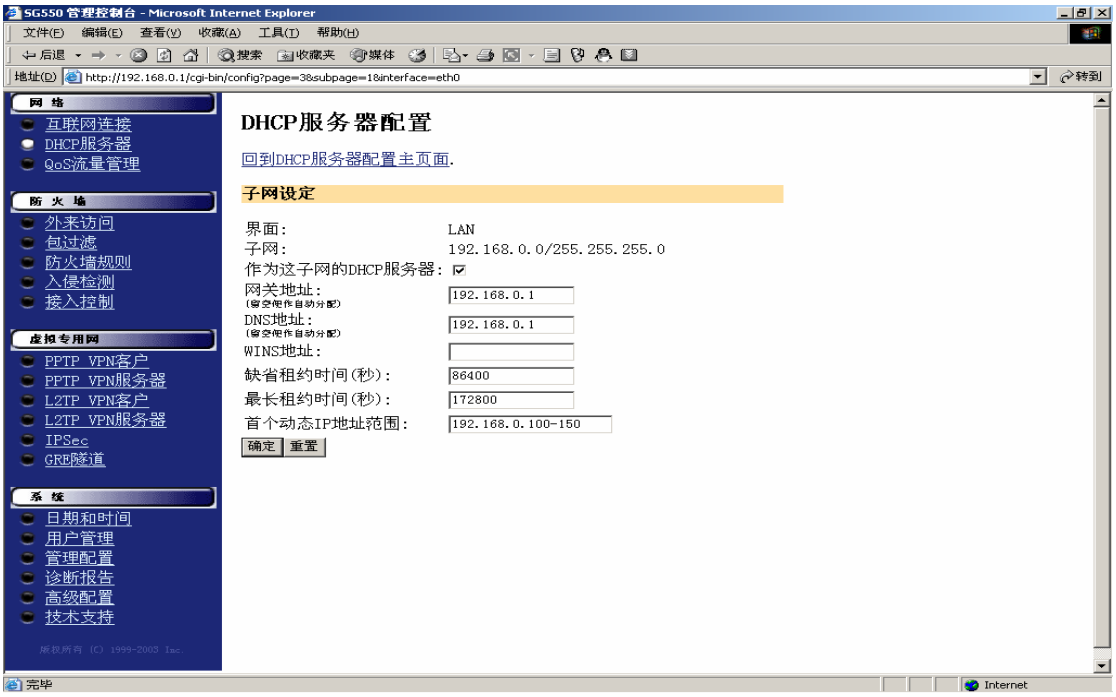


图 6-4

按 确定 按钮后：参看图 6-5

图 6-5

七、Cylan 防火墙配置

1、外来访问：

对进入 Cylan 的数据包做处理　参看图 7-1

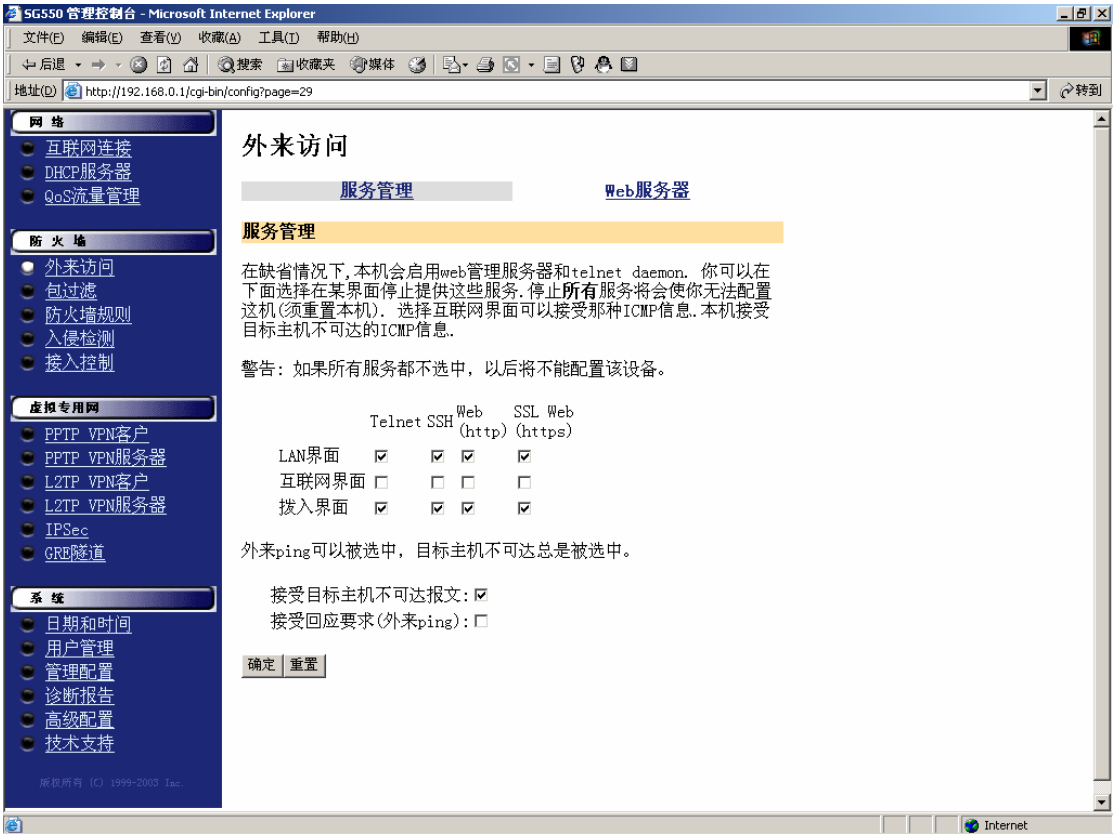


图 7-1

在图 7-1 中，Cylan 设备默认只能由 LAN 界面和拨入界面做管理，如果用户希望通过互联网对设备做远程管理，在图 7-1 中，互联网界面 对应的服务必须选中

Cylan 设备默认是不会响应 PING,如果要响应外来 PING,必须选中 接受回应要求

Cylan 设备默认是通过 HTTP 做管理配置的，如果用户需要使用 HTTPS,请按下面的步骤：
点击图 7-1 中　Web 服务器，如下图：

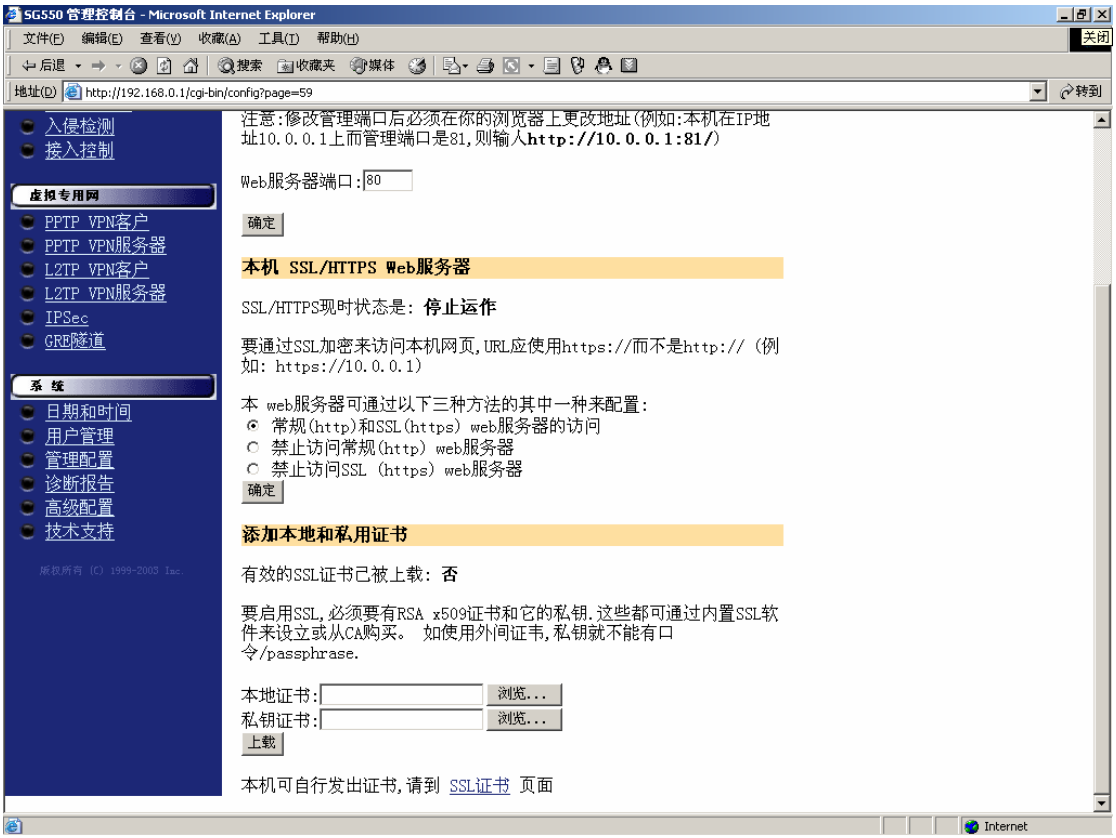


图 7-2

在图 7-2 中，点击 SSL 证书 进入下一步，如下图：

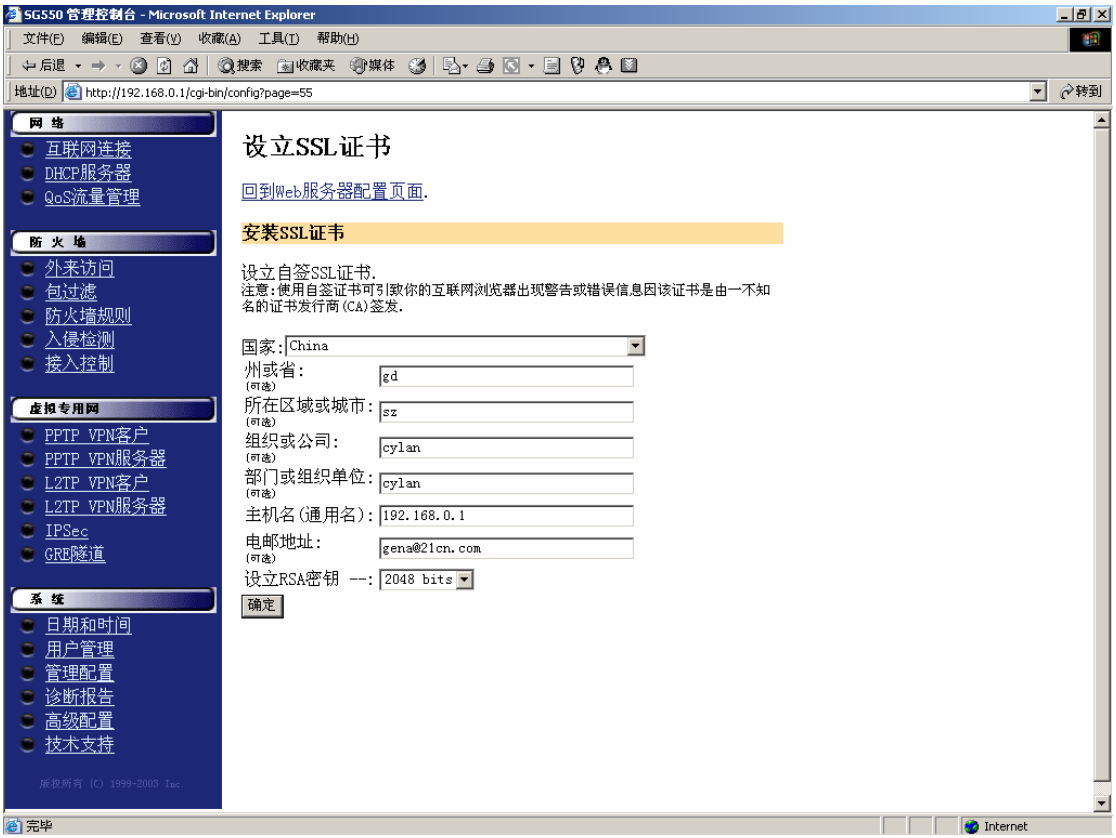


图 7-3

在图 7-3 中 点击 确定 ，生成一个证书，接着重起Cylan设备，输入https://192.168.0.1 回车，如下图：

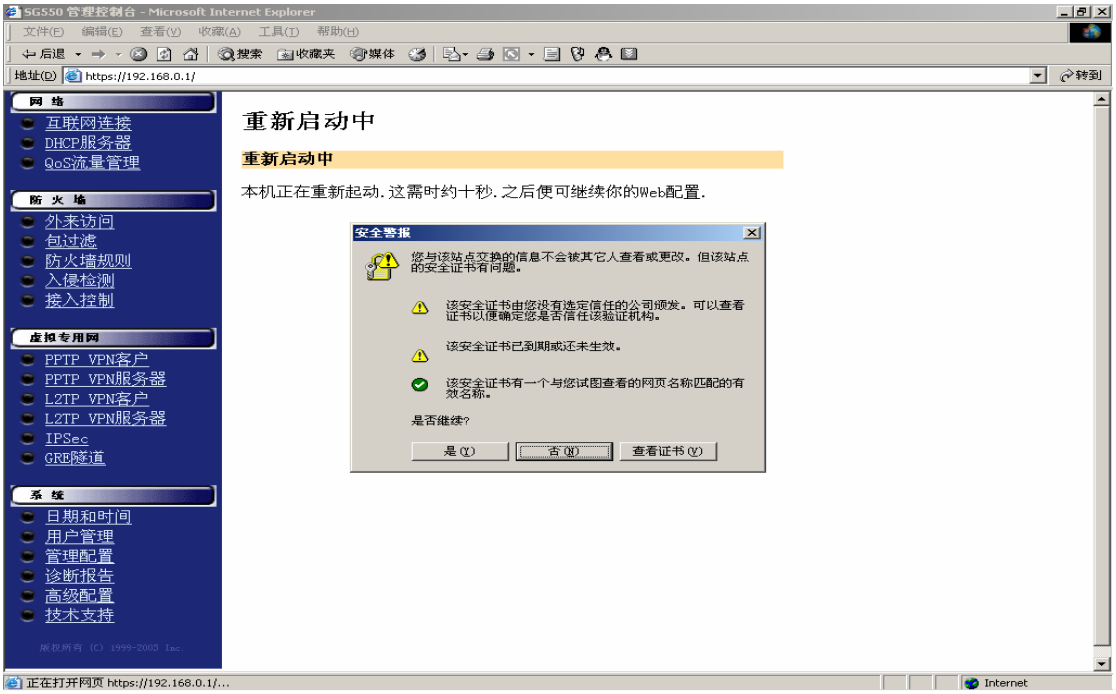


图 7-4

点击 “是 ”进入 Cylan 的配置界面，如下图

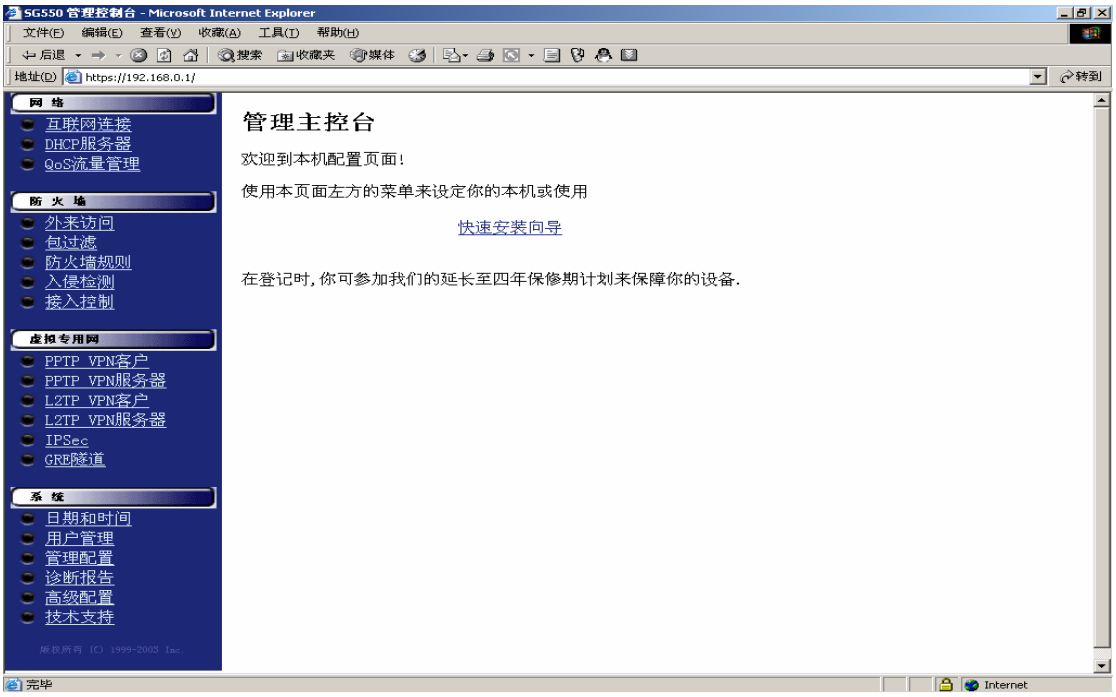


图 7-5

2、包过滤

Cylan 防火墙的默认策略如下表：

外进界面/接口	外出界面/接口	处理动作
LAN/VPN/Dial-In	**ANY**	接受
WAN	**ANY**	丢弃

在上表中，所有从 LAN/VPN/Dial-In 进入防火墙的数据，可以从任何接口出去
但所有从 WAN 进入防火墙的数据，不管去往那个接口，防火墙默认都会丢弃该数据

用户可以配置防火墙来控制网络流量，如基于源地址、目的地址、数据进入/出去的网络端口和应用服务等

用户可以配置防火墙的 NAT（网络地址转换），如源地址 NAT\目的地址 NAT\1 to 1NAT

在配置防火墙规则和 NAT 之前，用户必须先定义 IP 地址和服务组

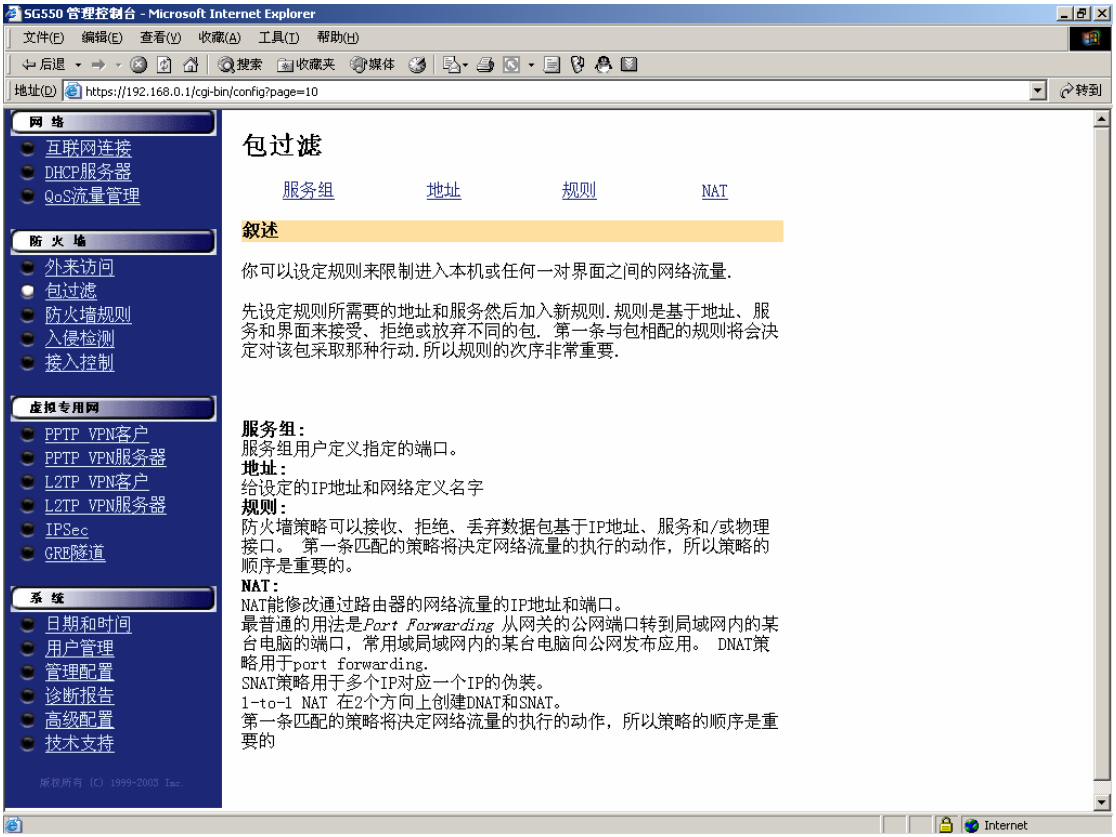


图 7-6

定义地址：

你可选用主机 DNS 名或 IP 地址来设定一个地址.

要用主机 DNS 名来设定一个地址,在名称栏填上主机 DNS 名和留空 IP 地址栏

要用 IP 地址来设定一个地址,填写 IP 地址栏.你可在名称栏填上该地址的简介或把它留空.

名称:www.cylan.com.cn

IP 地址: 210.51.168.69

确定 重置

用户可以定义 IP 地址（保留 IP 或公网 IP）;如果用户定义的是域名，那么 IP 地址可以不填（Cylan 设备会自动解析出域名对应的 IP）

服务组定义如下图：

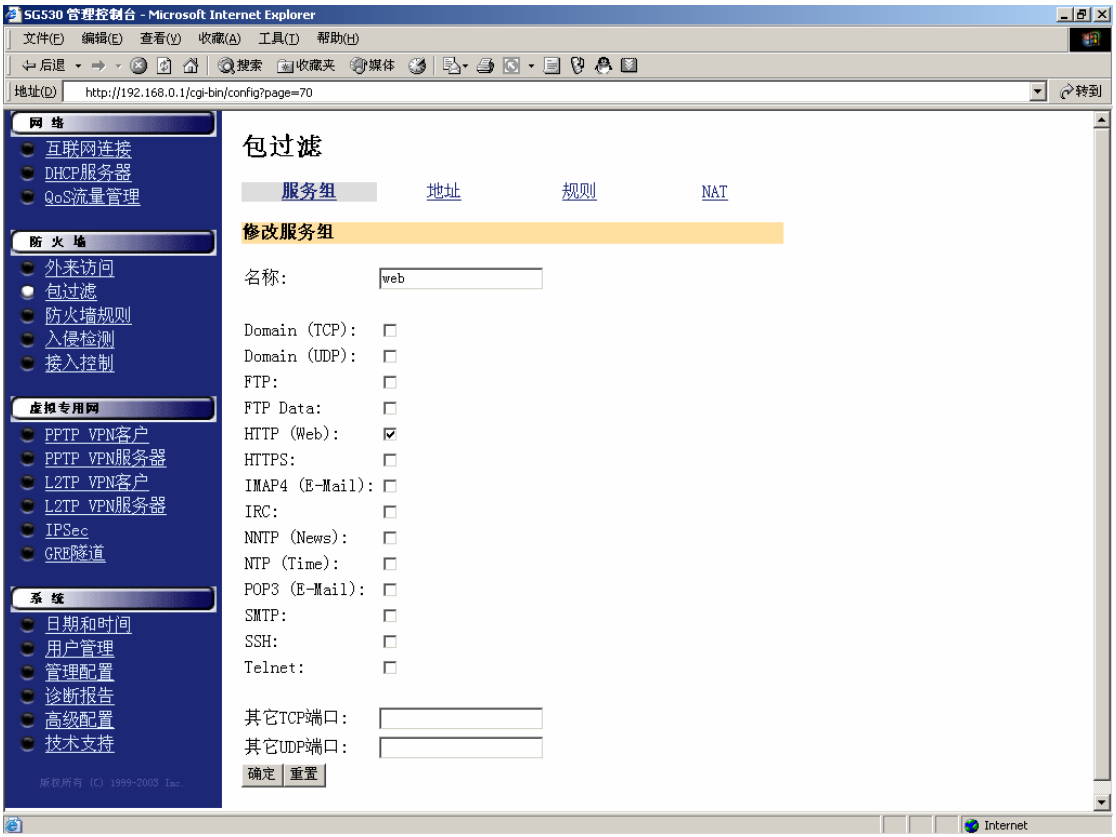


图 7-7

按 “确定 ” 进入 下一步

规则 定义如下图：

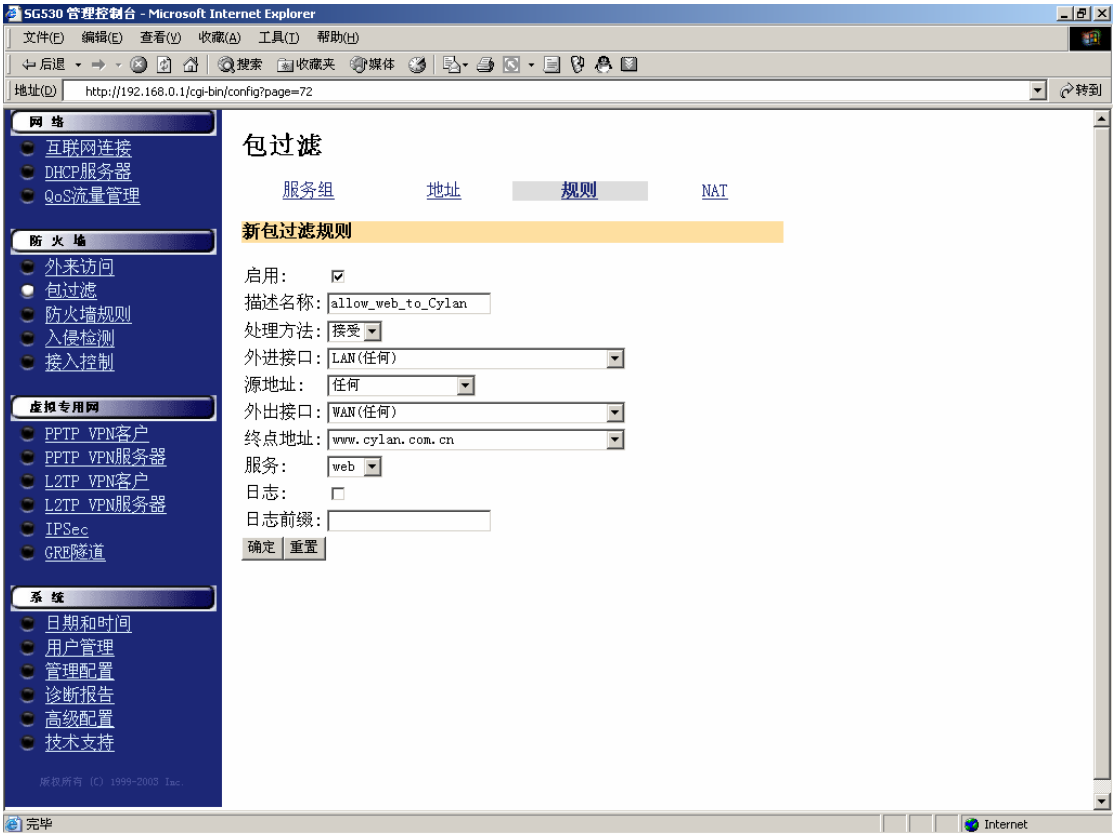


图 7-8

按“ 确定” 后，如下图：

图 7-9

注意：
进入防火墙数据首先匹配第一条规则，如果不匹配，数据将会和下一条匹配，直到有匹配的规则；所以防火墙规则的先后顺序很重要

NAT 配置（略）

在图 7-9 中，防火墙规则　　配置页如下：

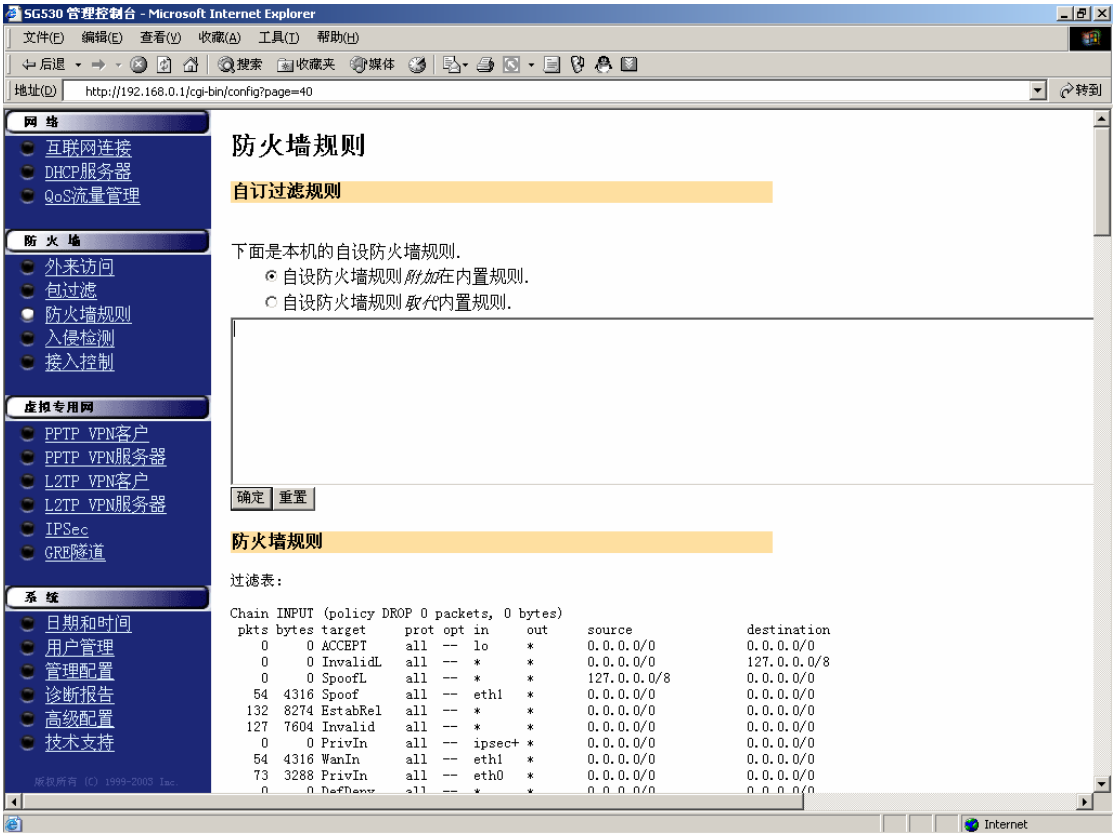


图 7-10

在图7-10中用户可以查找到已经添加的防火墙规则；如果用户对iptables比较熟悉，也可以在上图的方框中定义防火墙规则，有兴趣的用户可以浏览：
http://www.netfilter.org/documentation
iptables 配置示例：
1.关闭所有服务
iptables –A Filter –j DROP
2. 禁止某个 MAC 地址的某个端口服务
iptables -I Filter -p tcp -m mac --mac-source 00:20:18:8F:72:F8 --dport 8000 -j DROP
3. 禁止某个 IP 地址服务：
iptables –A Filter -p tcp -s 192.168.0.1 --dport 80 -j DROP
iptables –A Filter -p udp -s 192.168.0.1 --dport 53 -j DROP
4. 禁止某个 IP 地址的 PING:
iptables –A Filter –p icmp –s 192.168.0.1 –j DROP

5.将 WAN 口 NAT 到 PC

iptables -t nat -A PREROUTING -i $INTERNET_IF -d $INTERNET_ADDR -j DNAT --to-destination 192.168.0.1

6.禁用 QQ 防火墙配置

iptables -A Filter -p udp --dport ! 53 -j DROP

iptables -A Filter -p tcp -d 218.17.209.0/24 -j DROP

iptables -A Filter -p tcp -d 218.18.95.0/24 -j DROP

7.只允许某些服务，其他都拒绝

iptables -A Filter -p tcp -s 192.168.0.1 --dport 1000 -j ACCEPT

iptables -A Filter -j DROP

8.禁止某个 MAC 地址访问 internet:

iptables -I Filter -m mac --mac-source 00:20:18:8F:72:F8 -j DROP

9.拒绝某个地址多个端口服务

iptables -A Filter -p tcp -m multiport --destination-port 22,53,80,110 -s 192.168.20.3 -j REJECT

10.拒绝某段时间上网

iptables -A Filter -s 10.10.10.253 -m time --timestart 6:00 --timestop 11:00 --days Mon,Tue,Wed,Thu,Fri,Sat,Sun -j DROP

4、检测入侵（略）

请联系热线支持：0755-83233414 或 Email:support@cylan.com.cn

5、接入控制（略）

请联系热线支持：0755-83233414 或 Email:support@cylan.com.cn

八、Cylan VPN 配置

1、PPTP VPN 客户 配置 参看图 8-1

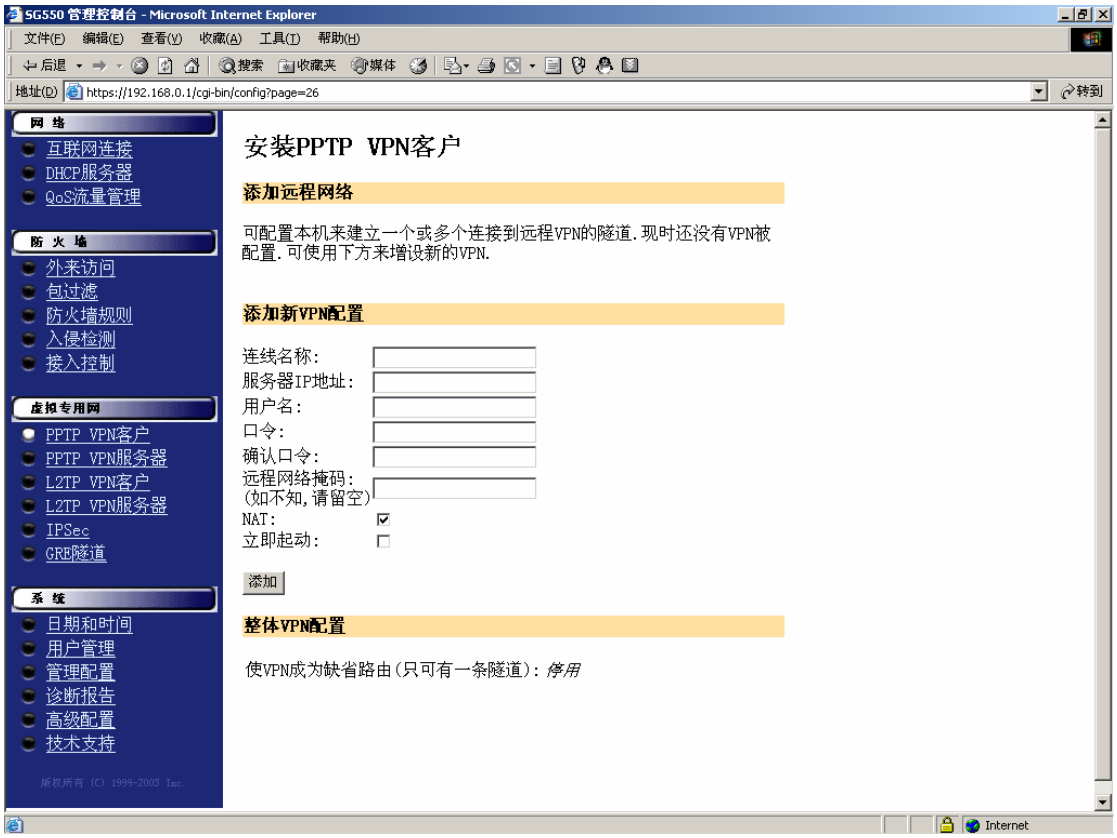


图 8-1

在图 8-1 中，用户操作如下：

连线名称: *用户指定*

服务器 IP 地址: *PPTP Server Internet 口的公网 IP*

用户名: *PPTP Client 账号*

口令: *口令*

确认口令: *口令确认*

远程网络掩码(如不知,请留空): *PPTP Server Lan 口的子网掩码*

NAT: *选中*

立即起动: *选中*

以上各项配置完后，按 添加 按钮添加新隧道连接！

2、PPTP VPN服务器 配置 参看图 8-2

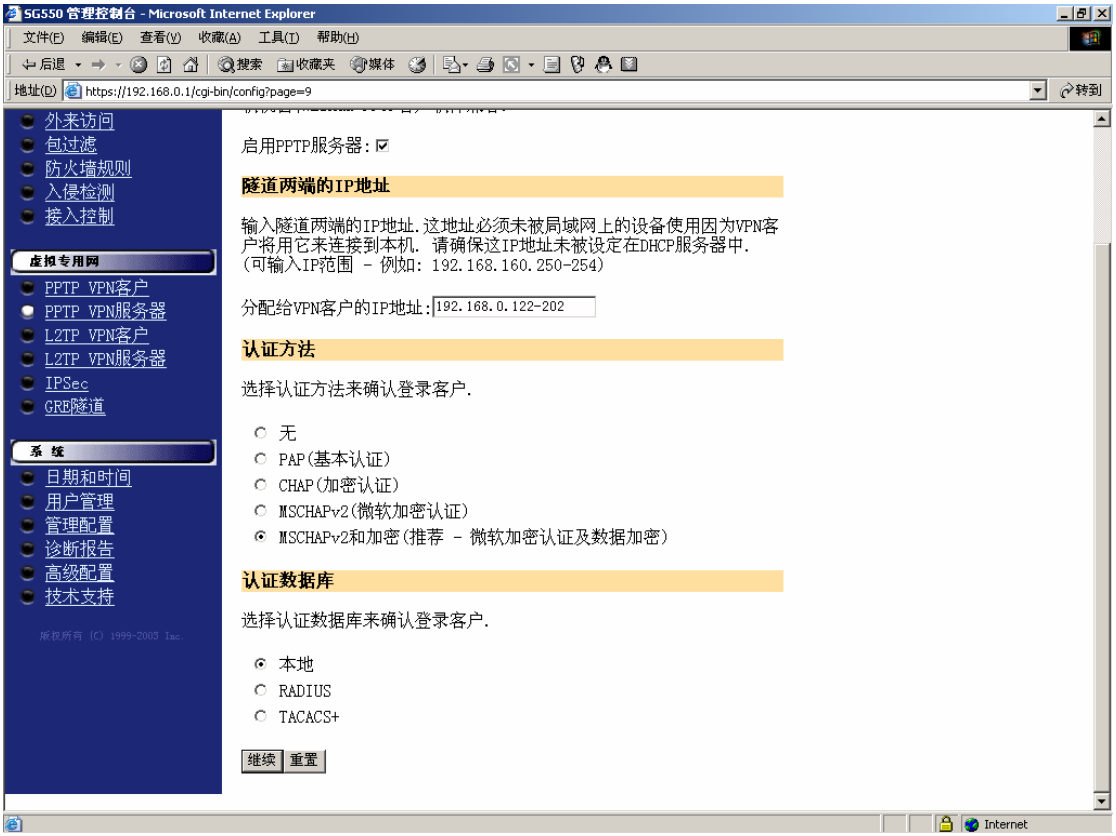


图 8-2

在图 8-2 中，用户操作如下：

Enable PPTP Server: *选中*

IP Address to Asign VPN Client: *PPTP Server 局域网内空闲的 IP 地址/自定 IP 地址*

Authentication Scheme： *选用 MSCHAPv2 and Encryption*

参数配置完后，按 继续 按钮进入 PPTP 账号配置！

PPTP Client 账号设置如图 8-3：

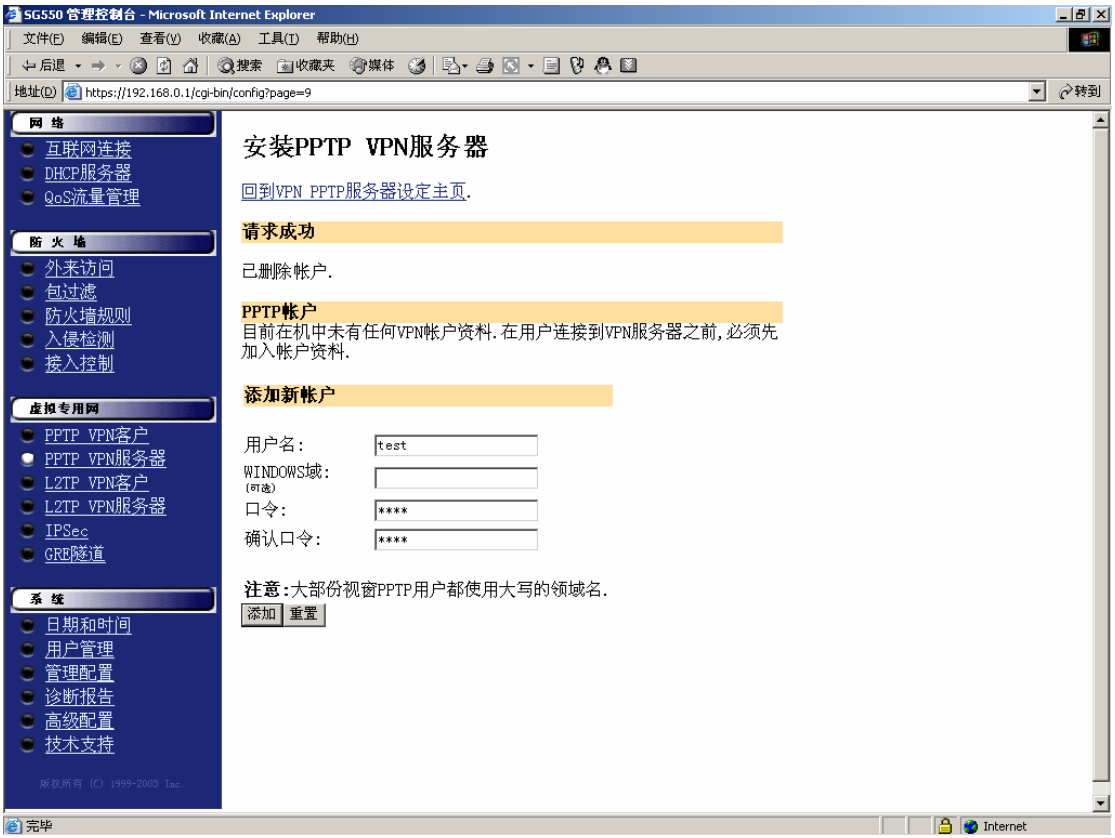


图 8-3

按　添加　进入下图：图中 test 为刚添加的 PPTP 帐号。

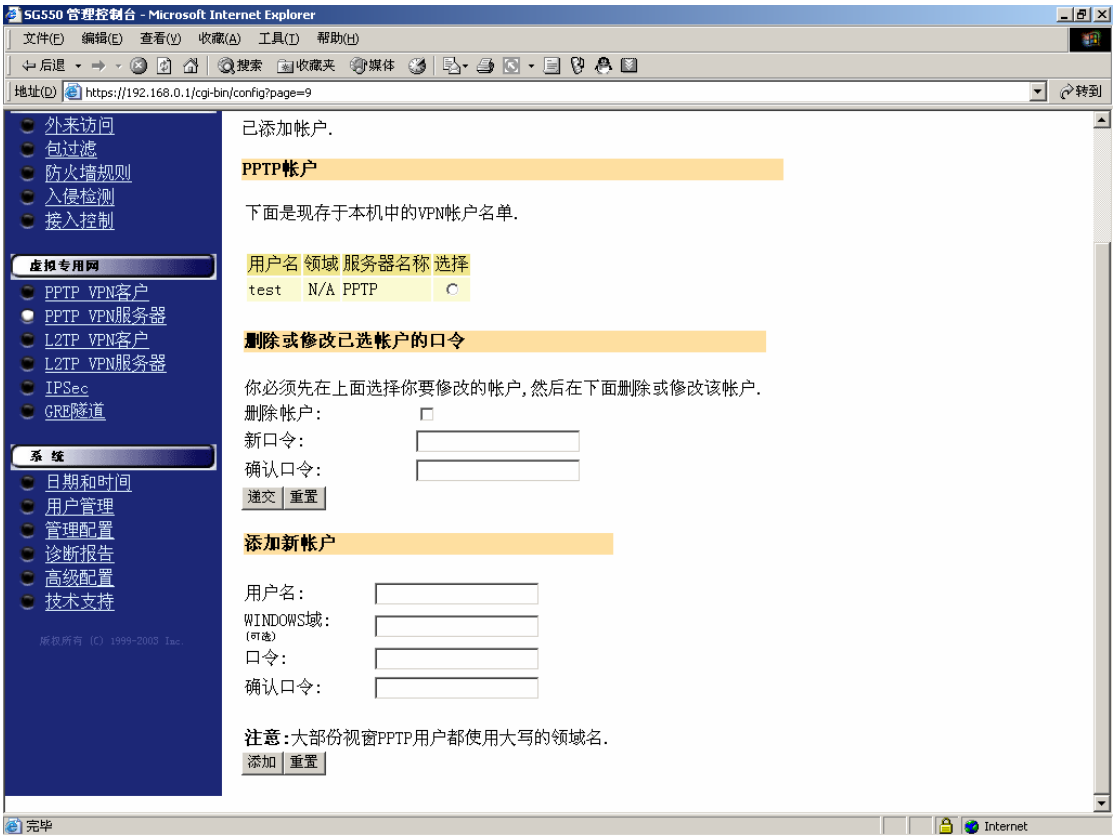


图 8-4

3、IPSEC 配置:

现以两台 CYLAN VPN （VPN1/VPN2）为例，做 IPSEC 隧道，

通用设定配置图例如下：

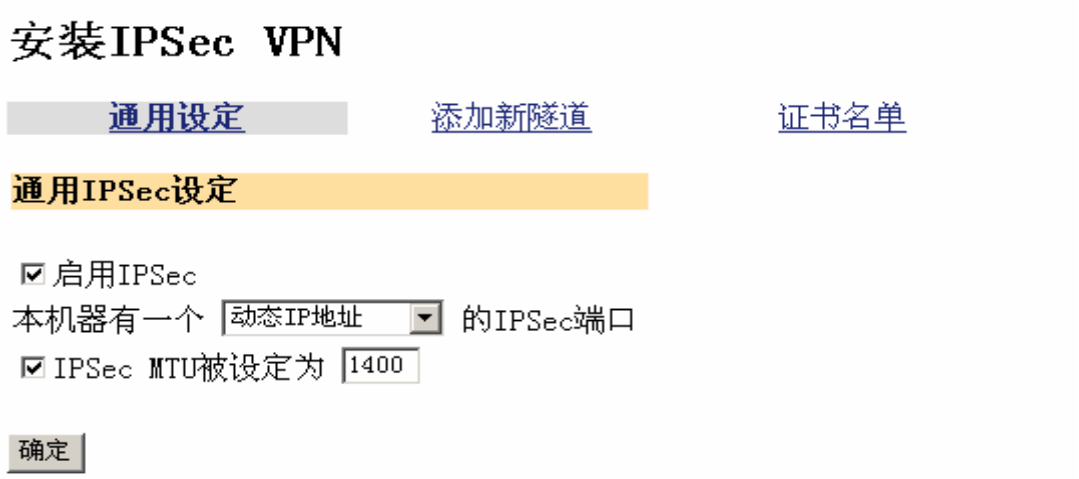


图 8-5

通用设定配好后，就可添加新隧道了。

VPN 1 IPSEC 配置图例如下:

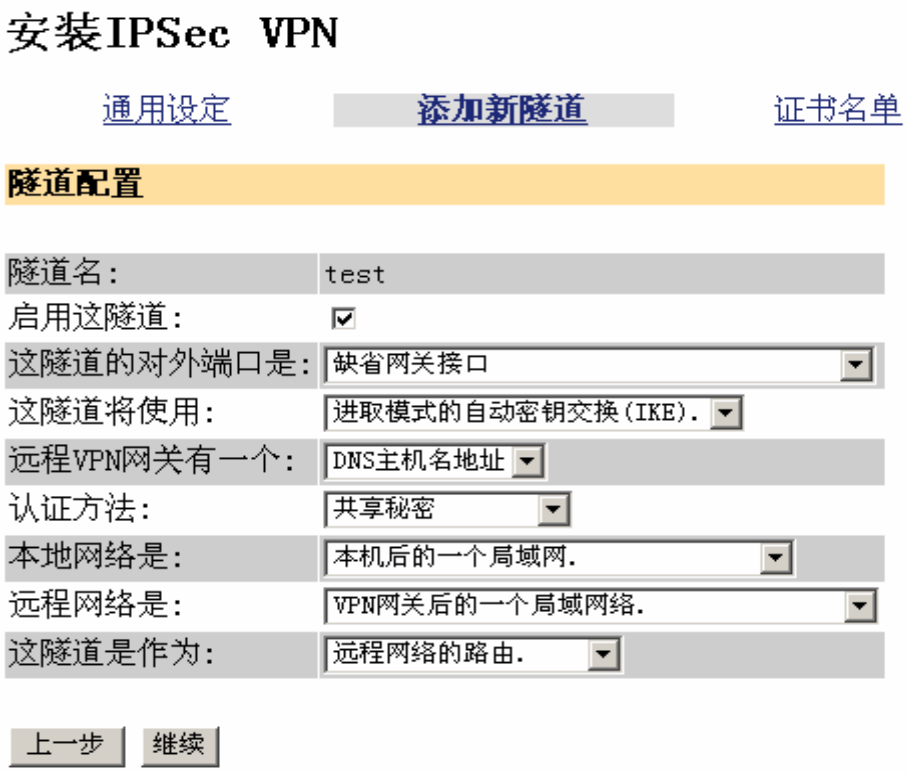


图 8-6

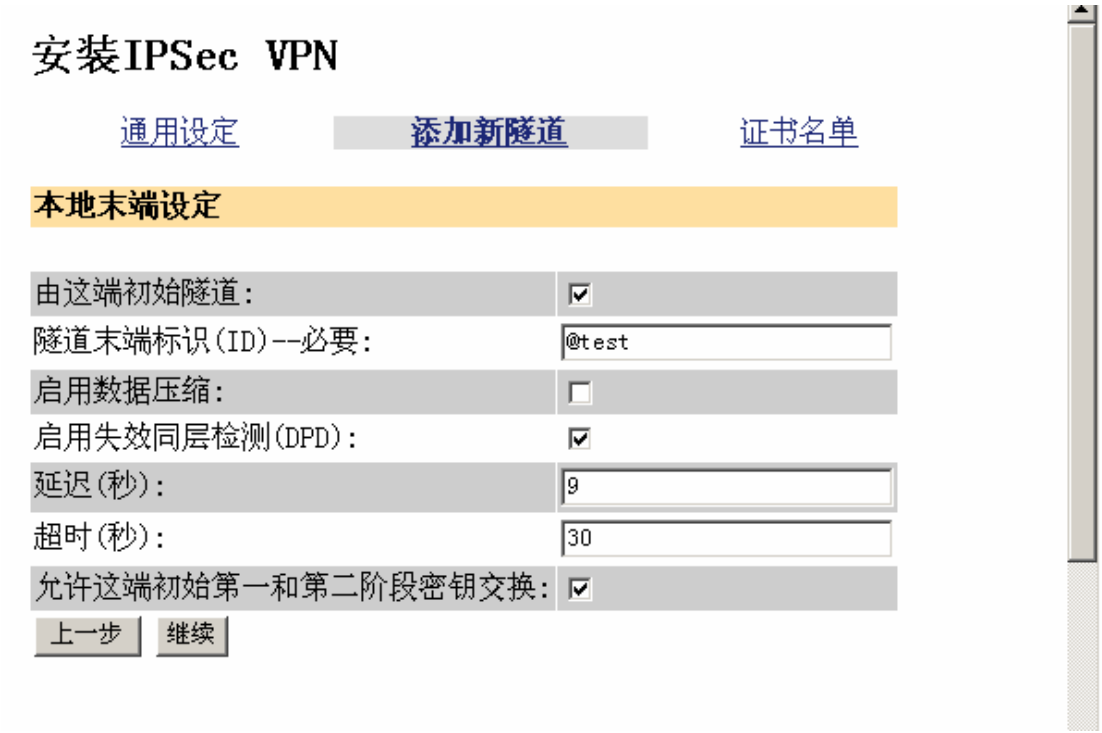

安装IPSec VPN
通用设定
添加新隧道
证书名单
本地末端设定
由这端初始隧道:
隧道末端标识(ID)--必要:
@test
启用数据压缩:
启用失效同层检测(DPD):
延迟(秒):
9
超时(秒):
30
允许这端初始第一和第二阶段密钥交换:
上一步
继续

图 8-7

安装IPSec VPN
通用设定
添加新隧道
证书名单
远程末端设定
远程VPN网关的DNS名:
cylan.3322.org
隧道末端标识(ID)--必要:
@test
上一步
继续

图 8-8

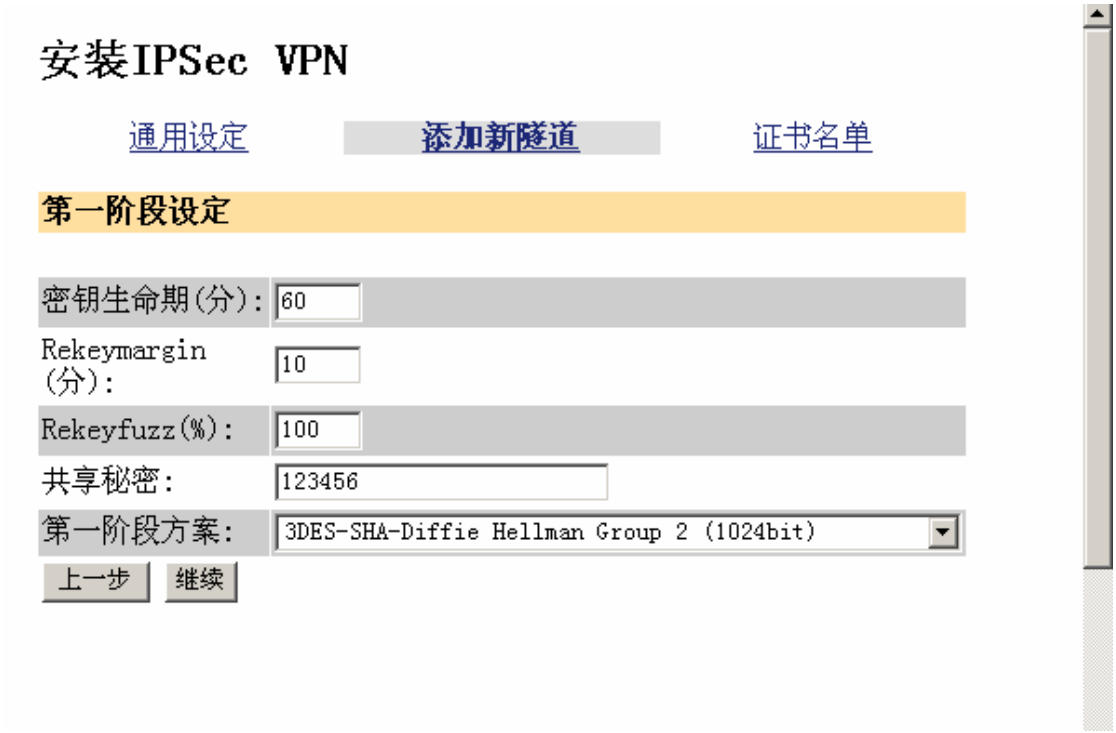

安装IPSec VPN
通用设定
添加新隧道
证书名单
第一阶段设定
密钥生命期(分):
60
Rekeymargin (分):
10
Rekeyfuzz(%):
100
共享秘密:
123456
第一阶段方案:
3DES-SHA-Diffie Hellman Group 2 (1024bit)
上一步
继续

图 8-9

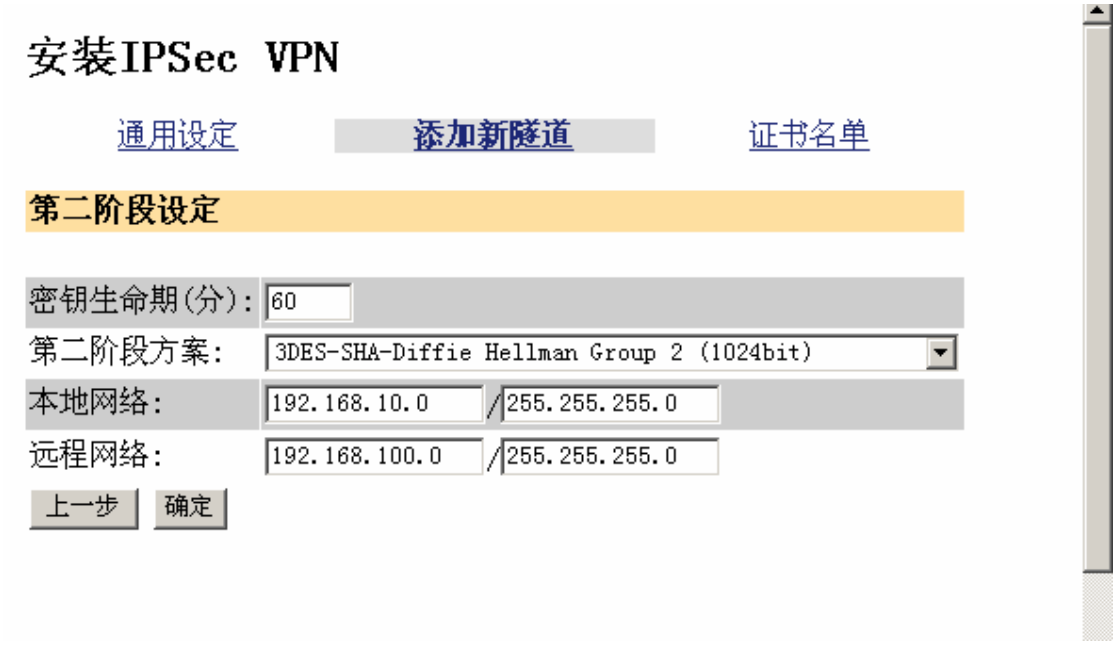

安装IPSec VPN
通用设定
添加新隧道
证书名单
第二阶段设定
密钥生命期(分):
60
第二阶段方案:
3DES-SHA-Diffie Hellman Group 2 (1024bit)
本地网络:
192.168.10.0
/255.255.255.0
远程网络:
192.168.100.0
/255.255.255.0
上一步
确定

图 8-10

VPN 2 IPSEC 配置图例如下:

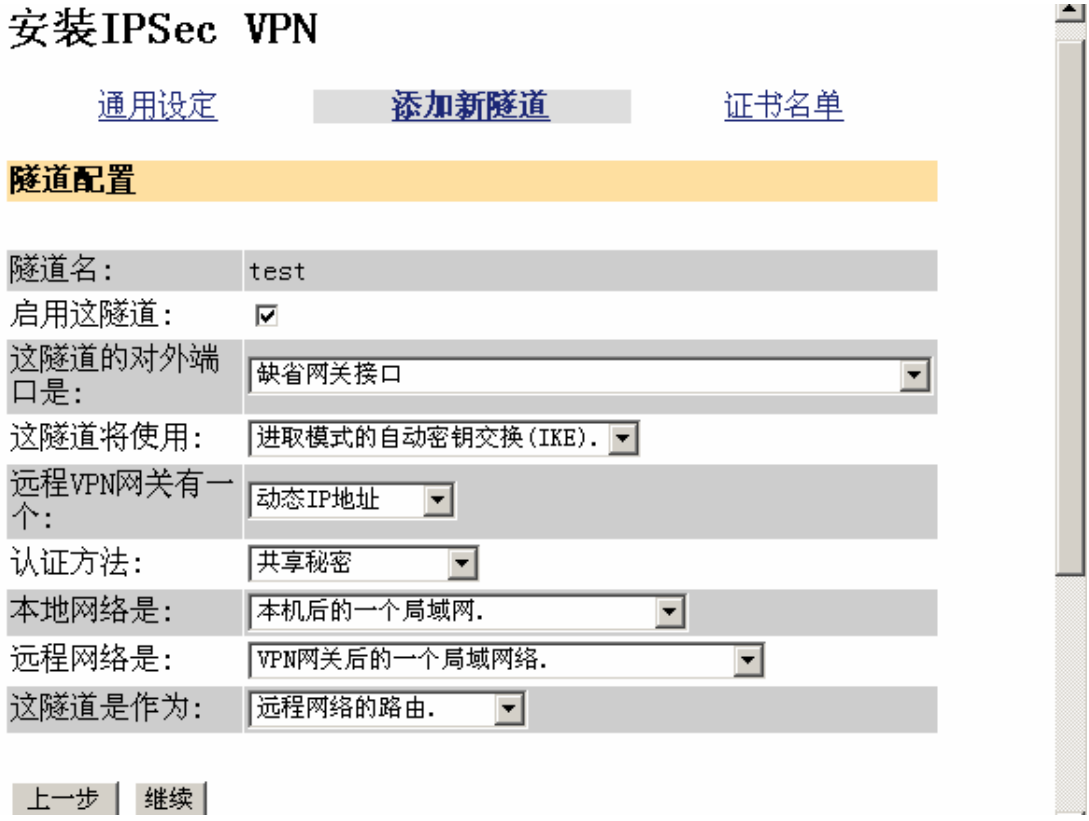


图 8-11

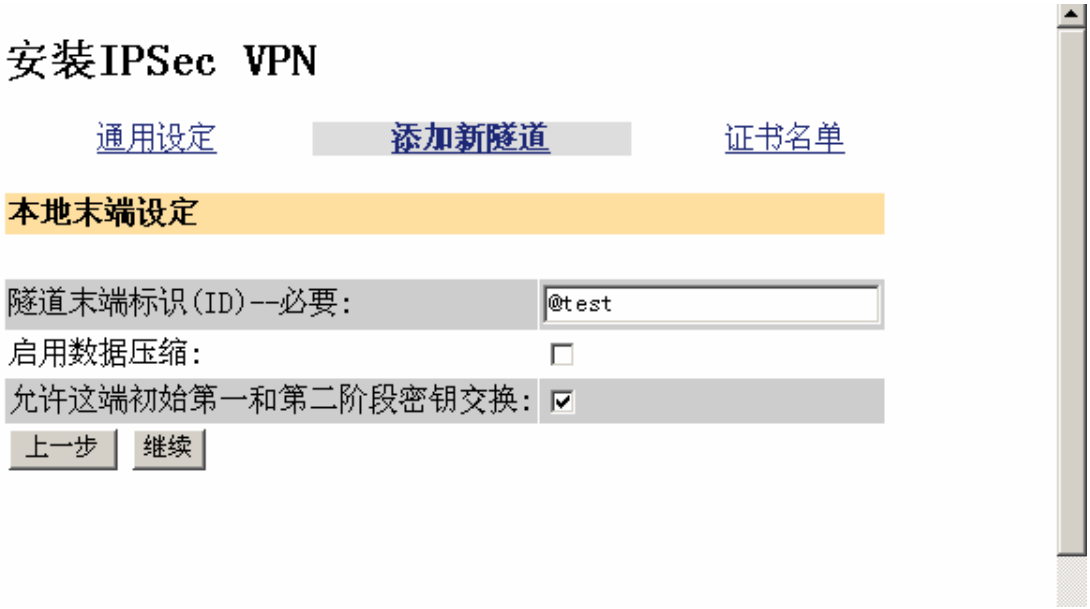


图 8-12

安装IPSec VPN
通用设定
添加新隧道
证书名单
远程末端设定
隧道末端标识(ID)--必要:
@test
上一步
继续

图 8-13

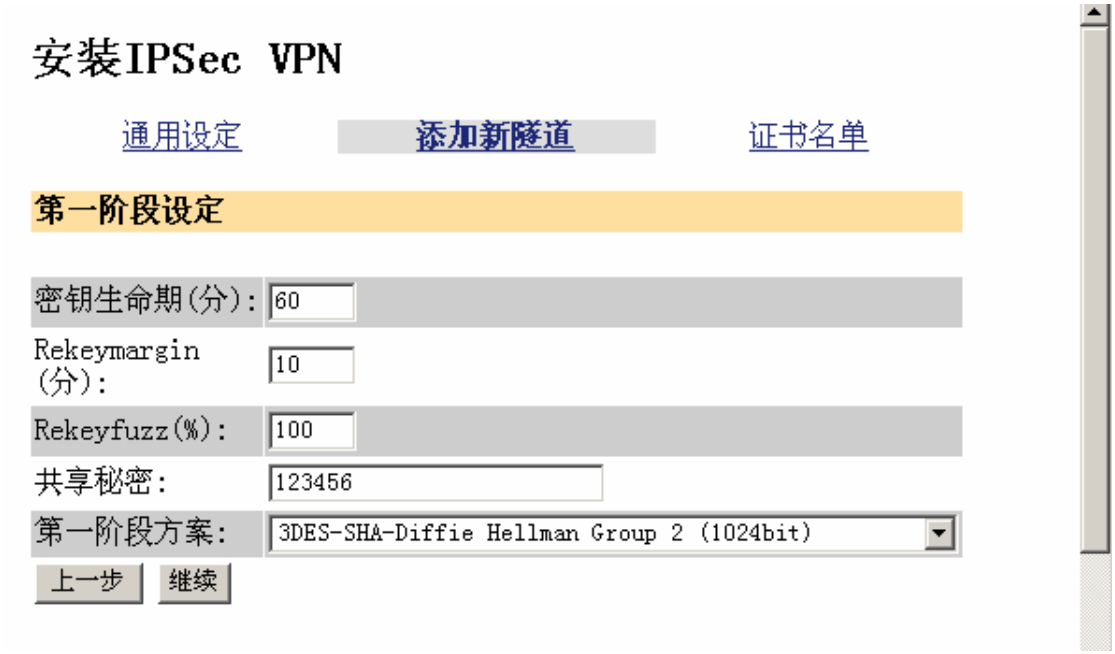

安装IPSec VPN
通用设定
添加新隧道
证书名单
第一阶段设定
密钥生命期(分):
60
Rekeymargin (分):
10
Rekeyfuzz(%):
100
共享秘密:
123456
第一阶段方案:
3DES-SHA-Diffie Hellman Group 2 (1024bit)
上一步
继续

图 8-14

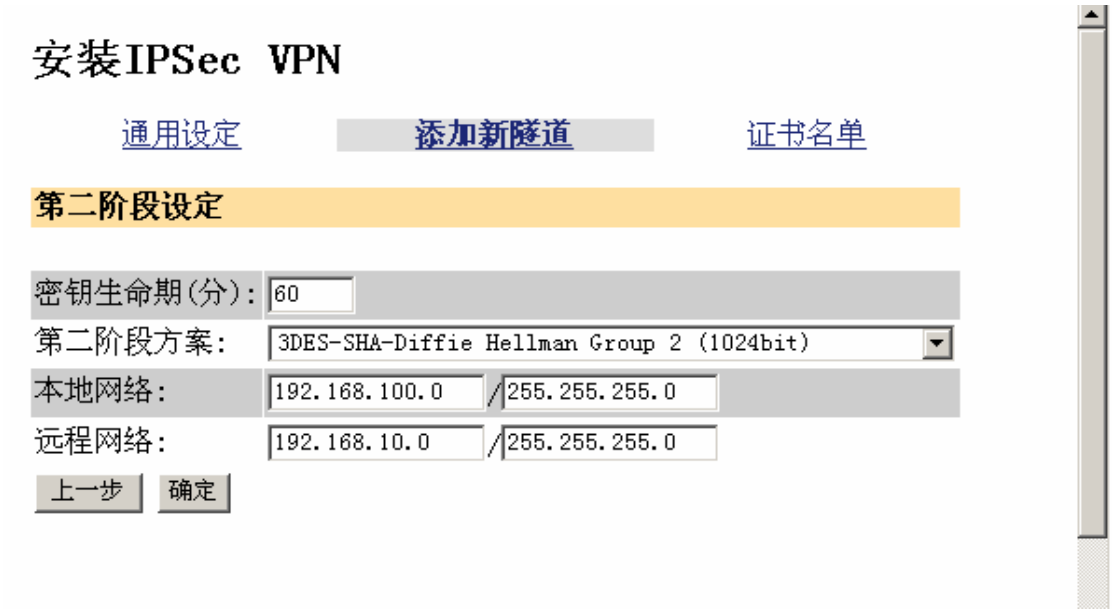


图 8-15

图 8-16

至此，IPSEC 隧道已建立，VPN1 和 VPN2 后面的两个网络可以互相访问了。
L2TP 配置和 PPTP 相同，请参考 PPTP 设置。
GRE 配置略。

九、Cylan 系统

1、日期和时间 参看图 9-1

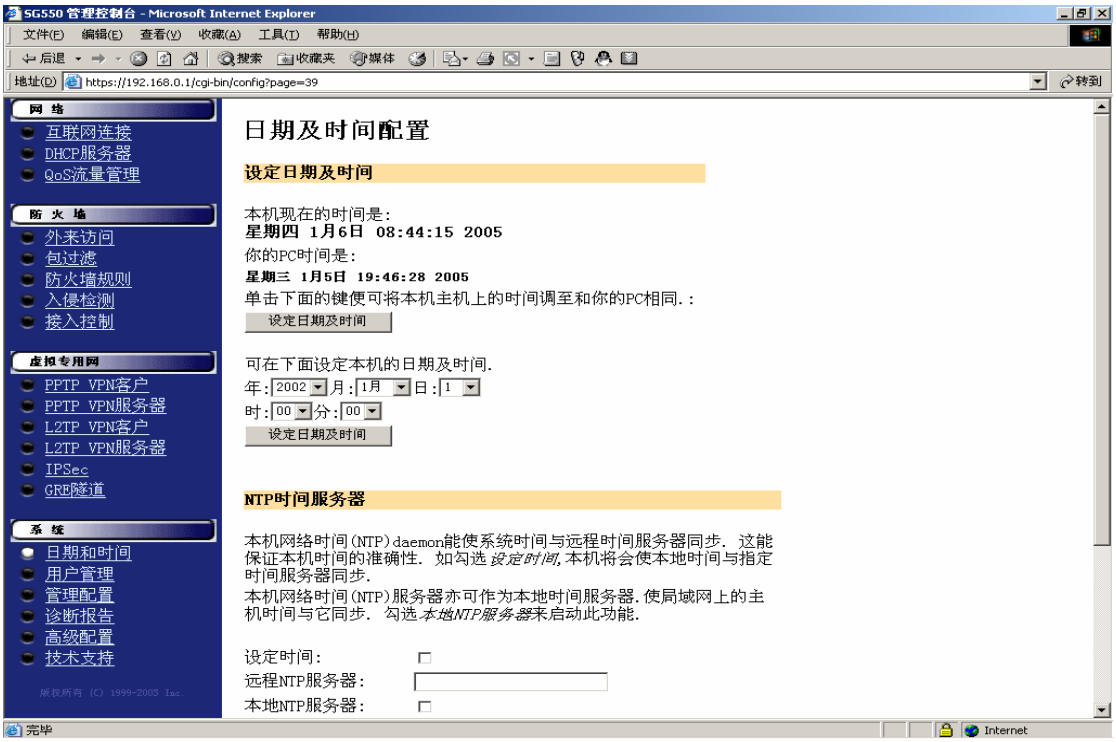


图 9-1

2、用户管理 参看图 9-2

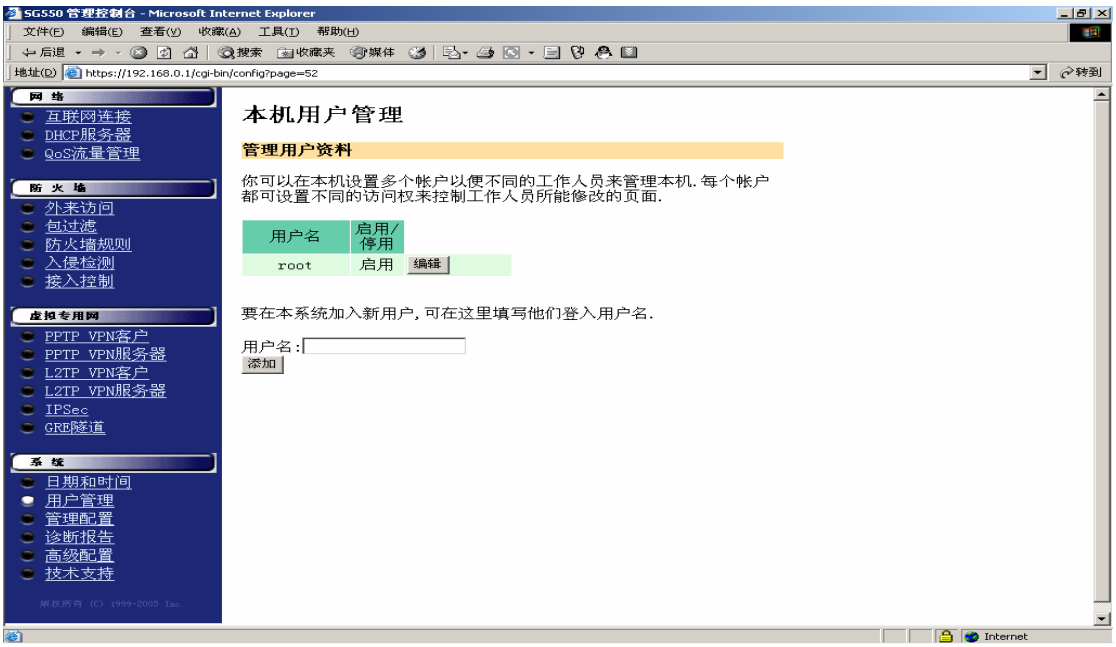


图 9-2

3、管理配置

参看图 9-3

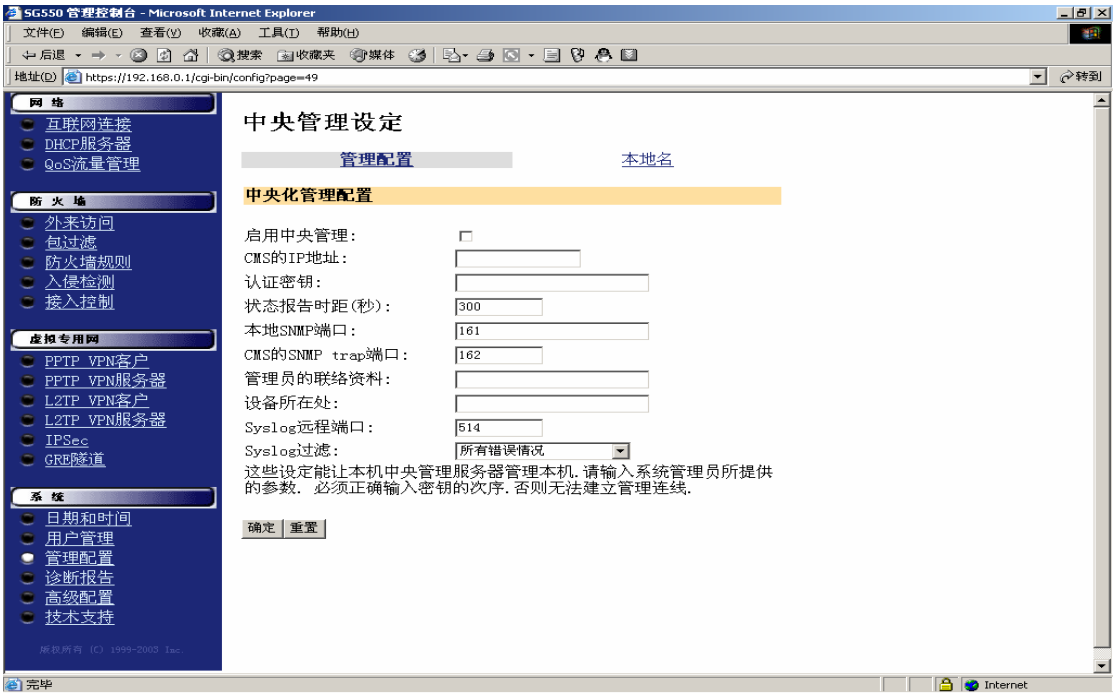


图 9-3

4、诊断报告　参看图 9-4

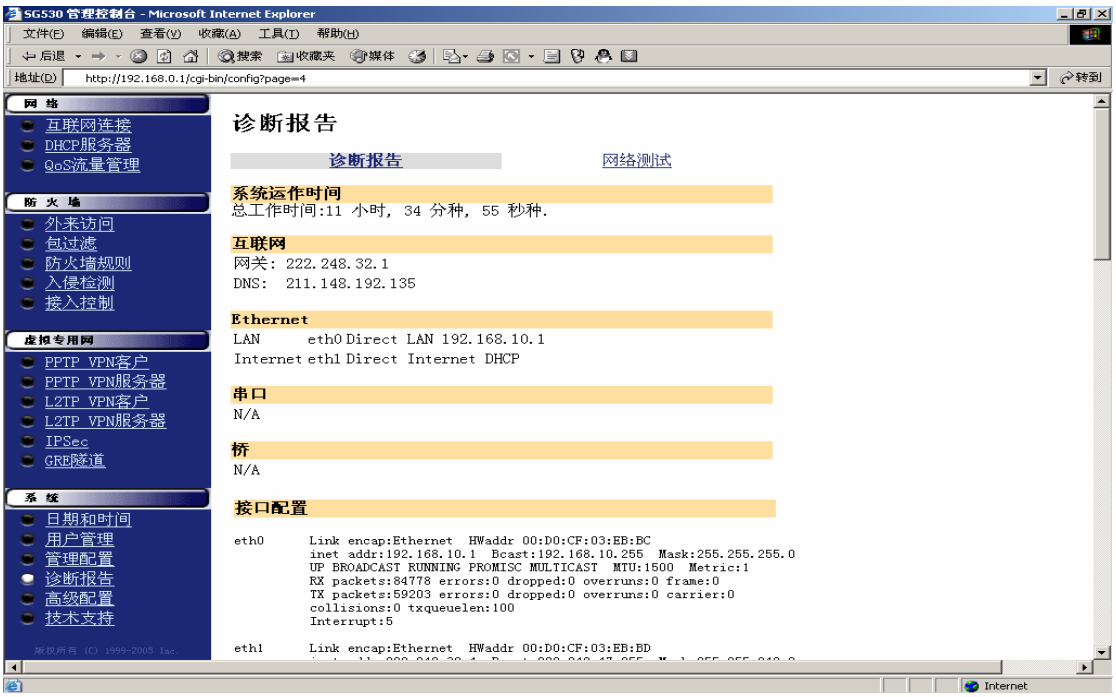
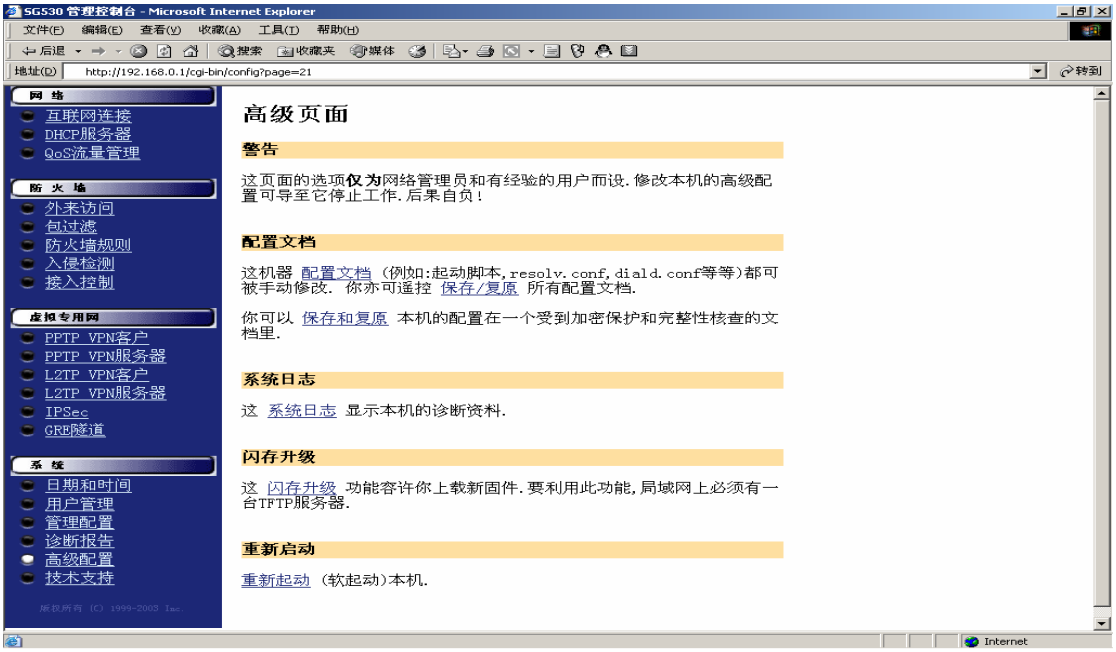
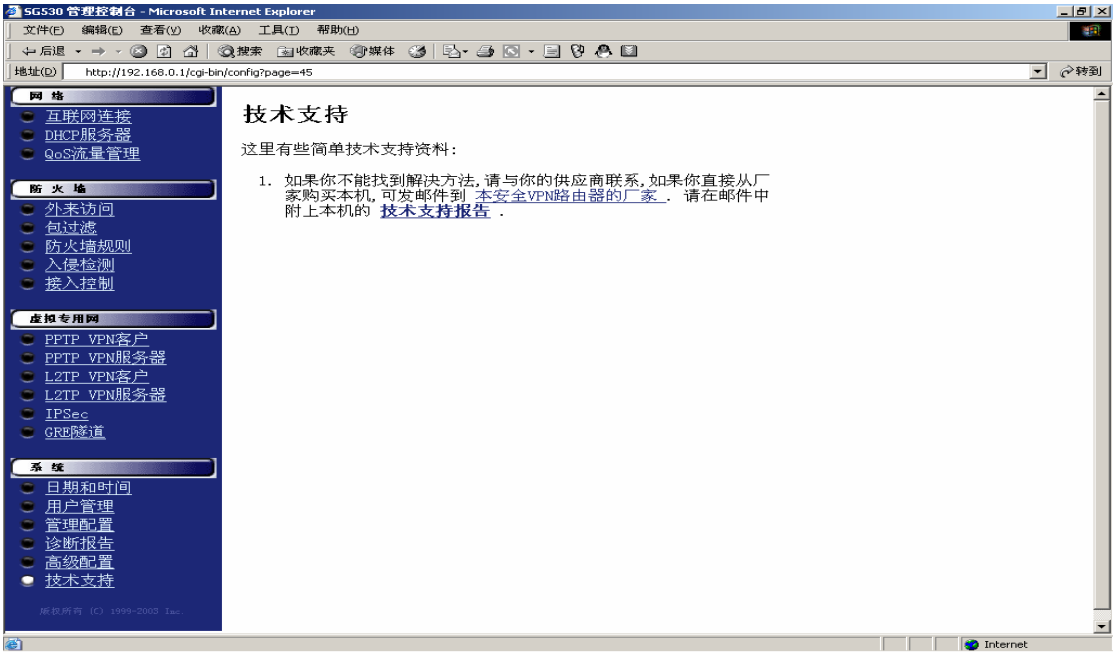


图 9-4

5、高级配置


SG530 管理控制台 - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
地址(D) http://192.168.0.1/cgi-bin/config?page=21
网络
互联网连接
DHCP服务器
QoS流量管理
防火墙
外来访问
包过滤
防火墙规则
入侵检测
接入控制
虚拟专用网
PPTP VPN客户
PPTP VPN服务器
L2TP VPN客户
L2TP VPN服务器
IPSec
GRE隧道
系统
日期和时间
用户管理
管理配置
诊断报告
高级配置
技术支持
高级页面
警告
这页面的选项仅为网络管理员和有经验的用户而设. 修改本机的高级配置可导至它停止工作. 后果自负!
配置文档
这机器 配置文档 (例如:起动脚本, resolv.conf, diald.conf等等)都可被手动修改. 你亦可遥控 保存/复原 所有配置文档.
你可以 保存和复原 本机的配置在一个受到加密保护和完整性核查的文档里.
系统日志
这 系统日志 显示本机的诊断资料.
闪存升级
这 闪存升级 功能容许你上载新固件. 要利用此功能, 局域网上必须有一台TFTP服务器.
重新启动
重新起动 (软起动)本机.
Internet

6、技术支持


SG530 管理控制台 - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
地址(D) http://192.168.0.1/cgi-bin/config?page=45
网络
互联网连接
DHCP服务器
QoS流量管理
防火墙
外来访问
包过滤
防火墙规则
入侵检测
接入控制
虚拟专用网
PPTP VPN客户
PPTP VPN服务器
L2TP VPN客户
L2TP VPN服务器
IPSec
GRE隧道
系统
日期和时间
用户管理
管理配置
诊断报告
高级配置
技术支持
技术支持
这里有些简单技术支持资料:
1. 如果你不能找到解决方法, 请与你的供应商联系, 如果你直接从厂家购买本机, 可发邮件到 本安全VPN路由器的厂家 . 请在邮件中附上本机的 技术支持报告 .
Internet

十、系统日志

点击　高级配置——〉系统日志，如图 10-1：

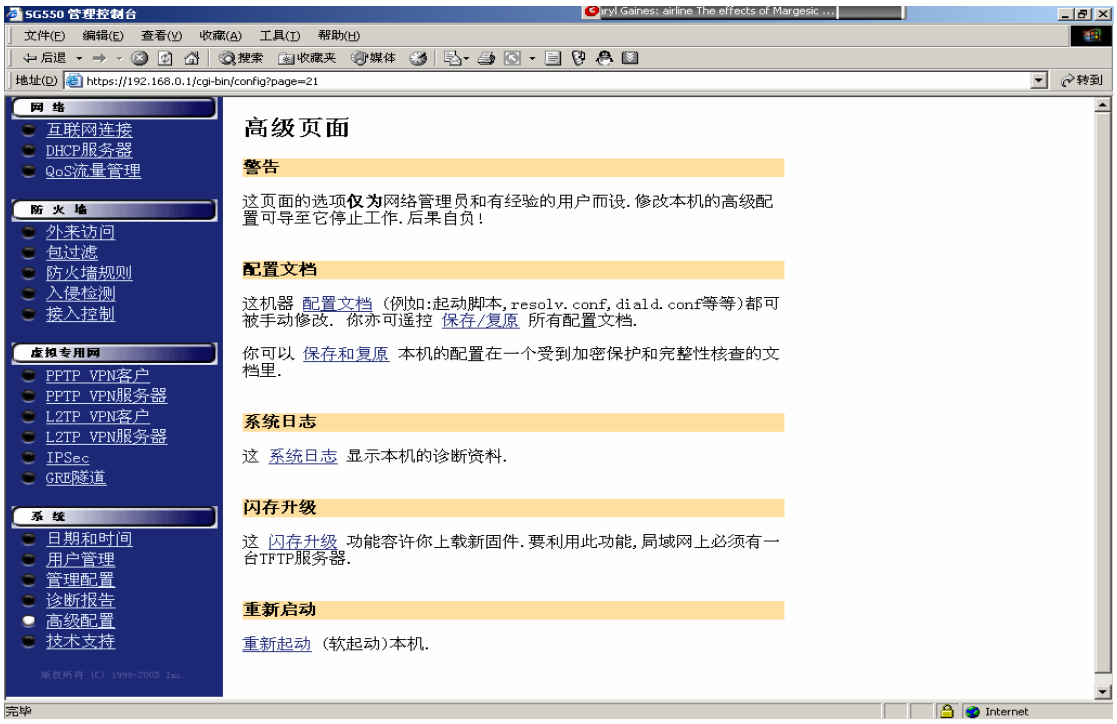


图 10-1

在图 10-1 中，点击　系统日志　如下图：

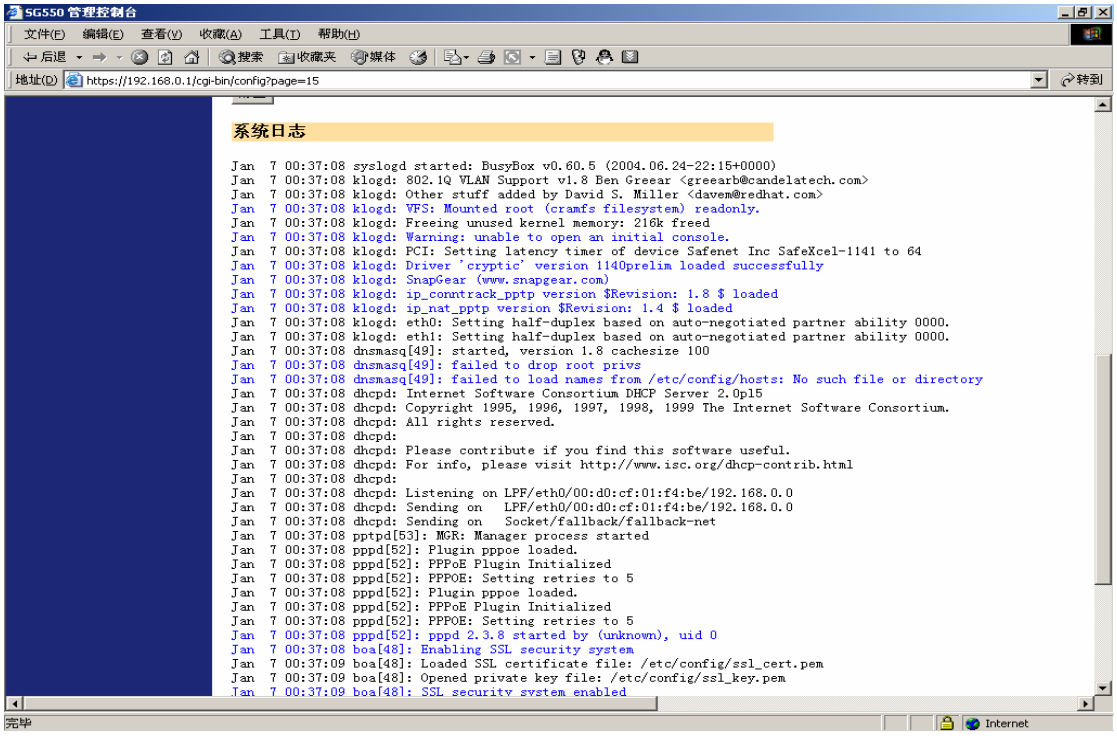


图 10-2

访问日志信息如下格式：

<*Date/Time*> klogd: <*prefix*> IN=<*incoming interface*> OUT=<*outgoing interface*> MAC=<*dst/src MAC addresses*> SRC=<*source IP*> DST=<*destination IP*> SPT=<*source port*> DPT=<*destination port*> <*additional packet info*>

举例如下：默认丢弃的数据日志信息（**Default deny**）

Mar 27 09:31:19 2003 klogd: Default deny: IN=eth1 OUT=MAC=00:d0:cf:00:ff:01:00:e0:29:65:af:e9:08:00 SRC=140.103.74.181 DST=12.16.16.36 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=46341 DF PROTO=TCP SPT=46111 DPT=139 WINDOW=5840 RES=0x00 SYN URGP=0

管理员访问日志如下：

Jan 7 00:46:53 boa[48]: Authentication attempt failed for root from 192.168.0.2 because: Bad Password
Jan 7 00:46:59 boa[48]: Authentication attempt failed for use from 192.168.0.2 because: Invalid Username
Jan 7 00:47:04 boa[48]: Authentication attempt failed for root from 192.168.0.2 because: Bad Password
Jan 7 00:47:19 boa[48]: Authentication successful for root from 192.168.0.2

当防火墙的用户名和密码不对时，防火墙会记录下登陆信息；

自定义日志：

iptables -I INPUT -j LOG -p tcp --syn -s <*X.X.X.X/XX*> -d <*Y.Y.Y.Y/YY*> --dport <*Z*> --log-prefix <*prefix*>

上面的命令是把**Internet** 发起的**tcp**连接，只要源地址是 ***X.X.X.X/XX* (-s ...)**和目的地址是***Y.Y.Y.Y/YY***, 且目的端口是 **Z**的数据就以**<*prefix*>** 名称记录在系统日志中；

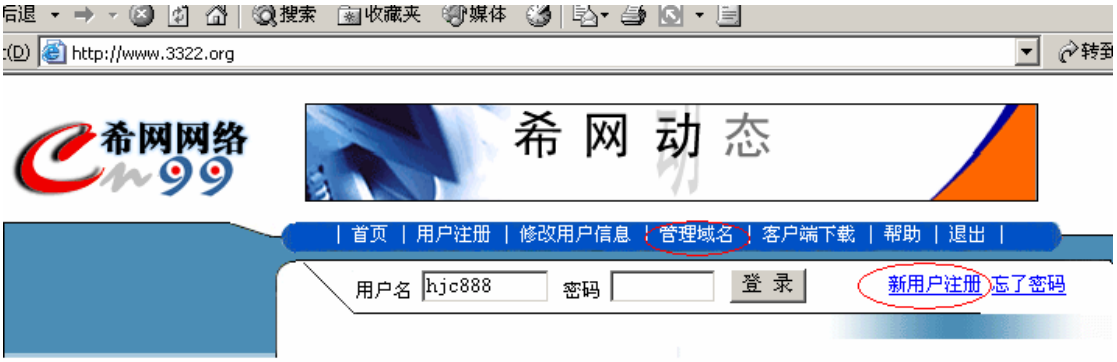
更为详细的信息请浏览**http://www.netfilter.org/documentation.**

十一、 Dynamic dns(动态域名解析)申请和使用

目前由于国内 IP 地址奇缺，因此申请有公网 IP 的上网方式，月租费用特别高，用这种方式组建 VPN，对于大部分公司来说是行不通的（费用太高）；目前 Adsl、各种宽带越来越普及，且上网的月租费用大多数公司都能承受，但是它的缺点就是没用静态 IP，用它组建 VPN 就比较麻烦，线路掉线后，必须重新建立 VPN 隧道（因为 IP 地址变了）；为了解决掉线后 IP 地址变了不方便建 VPN 隧道这个问题，我们引入了 Dynamic dns(动态域名解析),它解决了传统 DNS 解析必须是静态 IP 和域名的映射，引入了动态刷新机制；动态的 IP 和域名作一个动态的映射，对用户来说域名相当于静态 IP,建立 VPN 隧道时，使用域名就可以解决动态 IP 掉线重新建隧道的麻烦！

Cylan 设备目前支持多家提供动态域名服务的运营商，用户只需在运营商上申请一个账号就可以免费使用 Dynamic dns 服务。用户只要把申请到的账号输入 Cylan 设备中，以后用户一用 Cylan 设备上网，动态 IP 就会自动和域名做一个映射关系。

现以希网网络公司为例，动态域名申请步骤如下：



在 IE 地址栏里输入 http://www.3322.org 回车后，点击新用户注册，输入正确的信息后，用 EMAIL 收回密码并在首页登录，登录后点击管理域名--→动态域名--→新键,在主机名里输入你想申请的域名，如 cylan，点击确定后，即域名申请成功，你申请的域名为 cylan.3322.org，然后可在 VPN 上绑定这个域名，步骤如下：

点击 VPN 配置界面的互联网连接--→高级,找到动态 DNS 这一项，

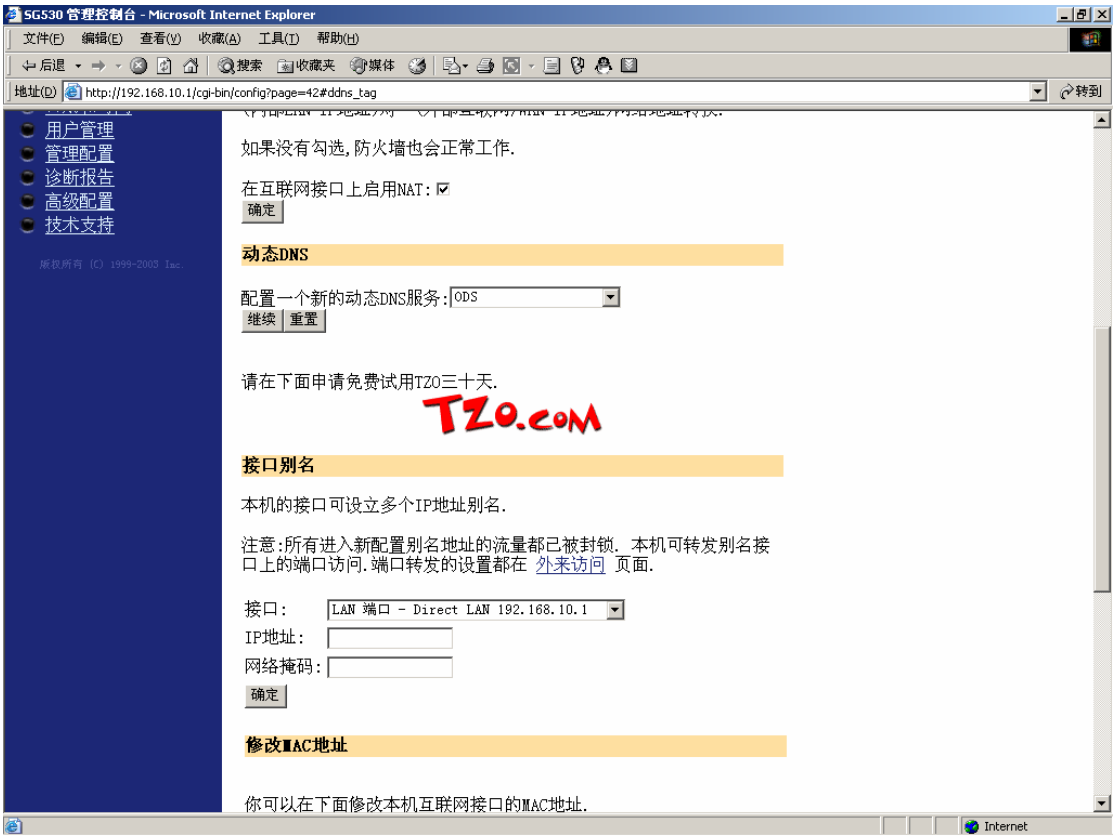


图 10-4

在图 10-4 中，选中 3322.org，接着按 继续 按钮进入下一步，如下图：

在上图中，输入对应的信息后，点击 确定 ，至此，动态域名已成功绑定。

附录：常见网络问题解决方法

序号	现象	解决方法
1	VPN 设备通电后前面板上的灯一直不停的闪，但不能访问到 192.168.0.1	在 3 秒中内按 VPN 设备后面板 Reset 按钮 2 次，等 20-30 秒后，再试着访问 192.168.0.1
2	VPN 设备的 Heartbeat/Tst 灯不闪	断电后重新起动 VPN 设备,如果通电后灯还不闪，请联系 VPN 设备供应商
3	VPN 通过 Adsl 上网掉线后，不能拨号上网	通常这种情况，您把 Adsl Modem 断电 5 分钟，再通电或和 Adsl 接入商联系，让他清除局端的 Adsl 进程，Modem 通常都能拨号；如还不能拨号，请和 VPN 设备供应商联系
4	用户忘了口令，VPN 无法进入配置界面	按 VPN 设备后面板的 Reset/Erase 键，恢复到出厂设置，重新配置设备就可以了
5	通电后，电源灯(Power LED)不亮	检查电源，电源如没问题，请联系 VPN 设备供应商

。

TEL：0755-83347282;

0755-83219335;

0755-83219315

E-Mail:support@cylan.com.cn

http://www.cylan.com.cn